

EXHIBIT 21



Go g e

[Chrome](#)

[Skip to content](#)

- [Features](#)
 - [Productivity](#)
 - [Google built-in](#)
 - [Security](#)
 - [Anywhere](#)
- [Do More with Chrome](#)
- [Extensions](#)
- [Enterprise](#)

Download [Chrome](#)

Go g e

[Chrome](#)

- [Features](#)
 - [Productivity](#)
 - [Google built-in](#)
 - [Security](#)
 - [Anywhere](#)
- [Do More with Chrome](#)
- [Extensions](#)
- [Enterprise](#)

Google Chrome Privacy Whitepaper

Last modified: March 12, 2019 (Current as of Chrome 73.0.3683.75)

- [Omnibox](#)
- [Network predictions](#)
- [Search locale](#)
- [New Tab page](#)
- [Tap to Search](#)
- [More like this](#)
- [Safe Browsing protection](#)
- [Unwanted software protection](#)
- [Navigation errors](#)
- [Offline Indicator](#)
- [Google update](#)
- [Network time](#)
- [Counting install](#)
- [Measuring promotions](#)
- [Usage stats](#)
- [Google Surveys](#)
- [Spelling suggestions](#)
- [Translate](#)
- [Signing In](#)
- [Autofill](#)
- [Payments](#)

- [Geolocation](#)
- [Speech to text](#)
- [Google Assistant](#)
- [Cloud Print](#)
- [SSL certificate error reporting](#)
- [Installed apps](#)
- [Push Messaging](#)
- [Chrome custom tabs](#)
- [Continue where you left off](#)
- [Chrome variations](#)
- [Do Not Track](#)
- [Plugins](#)
- [Media licenses](#)
- [Cloud policy](#)
- [Data Saver \(Chrome mobile\)](#)
- [Kid's Google Account](#)
- [Incognito and Guest mode](#)
- [Handoff support](#)
- [Security key](#)
- [Physical web](#)
- [Bluetooth](#)
- [Data sent by Android](#)

This document describes the features in Chrome that communicate with Google, as well as with third-party services (for example, if you've changed your default search engine). This document also describes the controls available to you regarding how your data is used by Chrome. Here we're focusing on the desktop version of Chrome; we touch only tangentially on Chrome OS and Chrome for Mobile. This document does not cover features that are still under development, such as features in the beta, dev and canary channel and active field trials, or Android apps on Chrome OS if Play Apps are enabled.

If you have questions about Google Chrome and Privacy that this document doesn't answer, please contact the privacy team at privacy@chromium.org. We'd be happy to hear from you.

Omnibox

Google Chrome uses a combined [web address and search bar](#) (we call it the "omnibox") at the top of the browser window.

As you use the omnibox, your [default search engine](#) can suggest addresses and search queries that may be of interest to you. These suggestions make navigation and searching faster and easier, and are turned on by default. They can be turned off by unchecking "Autocomplete searches and URLs" in the "Sync and Google services" section of Chrome's settings on desktop, and in the "Privacy" section of Chrome's settings on mobile. They are also disabled in incognito mode.



In order to provide these suggestions, Chrome sends the text you've typed into the omnibox, along with a general categorization (e.g., "URL", "search query", or "unknown"), to your default search engine. Chrome will also send a signal to your default search provider when you focus in the omnibox, telling it to get ready to provide suggestions. Your IP address and certain cookies are also sent to your default search engine with all requests, in order to return the results that are most relevant to you.

If Chrome determines that your typing may contain sensitive information, such as authentication credentials, local file names, or URL data that is normally encrypted, it will not send the typed text.

If Google is your default search engine, when you select one of the omnibox suggestions, Chrome sends your original search query, the suggestion you selected, and the position of the suggestion back to Google. This information helps improve the quality of the suggestion feature, and it's logged and anonymized in the same manner as Google web searches. Logs of these suggestion requests are retained for two weeks, after which 2% of the log data is randomly selected, anonymized, and retained in order to improve the suggestion feature.

If you've chosen to sync your Chrome history, and if Google is your default search engine, the URL of the page you're viewing is sent to Google in order to provide better, contextually relevant suggestions. URLs are sent only for HTTP pages and HTTPS pages, not other schemes such as file: and ftp:. Additionally, Chrome may present suggestions as soon as you place the cursor in the omnibox, before you start typing. Chrome is in the process of transitioning to a new service to provide these on-focus suggestions. For most users on desktop versions of Chrome, the request and complete set of suggestions are retained on Google servers in order to further improve and personalize the feature. When the URL that triggered the set of suggestions is deleted from your history, the set of suggestions will stop influencing suggestions personalized to you, and will be deleted; otherwise they are retained in your Google account for a year. For a small portion of users on desktop versions of Chrome, and users on mobile versions of Chrome, the logging described in the previous paragraphs apply except that URLs are never included in the 2% sampling of log data.

On Android, your location will also be sent to Google via an X-Geo HTTP request header if Google is your default search engine, the Chrome app has the permission to use your geolocation and you haven't blocked geolocation for www.google.com (or country-specific origins such as www.google.de). Additionally, if your device has network location

enabled (High Accuracy or Battery Saving Device Location mode in Android settings), the X-Geo header may also include visible network IDs (WiFi and Cell), used to geocode the request server-side. The X-Geo header will never be sent in Incognito mode. HTTPS will be required to include this header in the request. You can learn more about how to control the Android OS location sharing with apps on [this article](#) for Nexus, or find your device [here](#) if you do not use a Nexus. How to control location sharing with a site within Chrome is written in [this article](#). See the [Geolocation](#) section of this whitepaper for more information on default geolocation permissions.

Additionally, if Google is your default search engine and you have enabled sync, omnibox may also show suggestions for your Google Drive files. You can turn this functionality off by disabling the “Drive suggestions” option in the “Sync and Google services” section of Chrome’s settings.

If you use a non-Google search provider as your default search engine, queries are sent and logged under that provider's privacy policy.

Additionally, when you use the omnibox to search for a single word, Chrome may send this word to your DNS server to see whether it corresponds to a host on your network, and may try to connect to the corresponding host. This gives you the option to navigate to that host instead of searching. For example, if your router goes by the hostname “router”, and you type “router” in the omnibox, you’re given the option to navigate to <https://router/>, as well as to search for the word “router” with your default search provider. This feature is not controlled by the “Use a prediction service to help complete searches and URLs...” option because it does not involve sending data to your default search engine.

Network predictions

Chrome uses a prediction service to load pages more quickly. The prediction service uses navigation history and local heuristics to predict which resources and pages are likely to be needed next, and it initiates actions such as DNS prefetching, TCP and TLS preconnection, and prefetching of web pages. To [turn off](#) network predictions, uncheck “Use a prediction service to load pages more quickly” in the “Privacy” section of Chrome’s settings.

To improve load times, the browser can be asked to prefetch links that you might click next. Chrome supports four types of prefetching:

- Chrome prefetching - can be initiated by Chrome itself whenever it detects a search query typed in the omnibox or a likely beginning of a URL you type often
- Webpage prefetching - requested by one web page to prefetch another
- AMP prefetching - can be requested only by the Google Search App on Android to prefetch several accelerated mobile pages (AMP) articles and display them later in a Chrome Custom Tab
- CustomTabs prefetching - any Android app can request to prefetch several URLs to speed up displaying them later in a Chrome Custom Tab

Controlling the feature. All prefetching types except webpage prefetching are controlled by Chrome’s prediction service setting. Webpage prefetching is allowed regardless of whether Chrome’s network prediction service feature is enabled.

Handling of cookies. The prefetched site is allowed to set and read its own cookies just as if you had visited it (even if you don’t end up visiting the prefetched page). All types of prefetching are disabled if you disallow third party cookies to prevent cookies from being set from pages that you did not visit.

Javascript execution. For AMP prefetching the page is fully rendered and Javascript is also executed. For the remaining types of prefetching Javascript is not executed.

Google search locale

If Google is set as your default search engine, Chrome will try to determine the most appropriate locale for Google search queries conducted from the [omnibox](#) in order to give you relevant search results based on your location. For example, if you were in Germany, your omnibox searches may go through google.de instead of google.com.

In order to do this, Chrome will send a request to google.com each time you start the browser. If you already have any cookies from the google.com domain, this request will also include these cookies, and is logged as any normal HTTPS request to google.com would be (see the [description](#) of “server logs” in the [privacy key terms](#) for details). If you do not have any cookies from google.com, this request will not create any.

New Tab page

The Chrome New Tab page may display suggestions for websites that you might want to visit.

In order to help you get started, Chrome may suggest content that is popular in your country or region. Chrome uses your IP address to identify your country or region.

Chrome tries to make personalized suggestions that are useful to you. For this, Chrome uses the sites you have visited from your local browsing history. On Android, the most popular languages of the sites you visited may also be sent to Google to provide suggestions in languages you prefer to read, and the device display DPI may be sent to format content for your device. To save data, Chrome may additionally send a hash of the content that Google provided to you the last time, so that you only download content when there is something new.

If you are signed into Chrome, suggestions are *also* based on data stored in your Google account activity. You can control the collection of data in your Google account at [Activity controls](#) and manage your account activity at [My](#)

Activity. For example, if you sync your browsing history and have enabled its use in your Web & App activity, Google may suggest sites that relate to sites you have visited in the past. Chrome measures the quality of suggestions by sending Google information about the sets of suggestions that were displayed, and those that were selected.

On the desktop version of Chrome, you may also manually add shortcuts to websites that you regularly visit, or edit Chrome's existing website suggestions. After you add, edit, or delete a shortcut to a website, the Chrome New Tab page will not suggest any new websites to you.

Suggestions generated from your browsing history will be removed once you clear your browsing history. However, if you customized your suggestions, they will not be removed.

For Chrome on Android, in certain countries, Chrome may download the content of the New Tab page suggestions from Google, for use while offline. Chrome sends to Google a cookieless request with the URL for each suggestion, along with Chrome's user agent string, in order to render the content. You can remove downloaded content by clearing Chrome's cache data, or by opening the Downloads menu and selecting individual pages to delete. You can disable this feature by disabling "Automatically download pages" in Chrome's Privacy settings.

For desktop and Android versions of Chrome, when you open a new tab, Chrome loads a New Tab page customized by your default search engine (e.g., google.com) if it's available. This page is preloaded in the background and refreshed periodically so that it opens quickly. Your IP address and cookies, as well as your current browser theme, are sent to your search engine with each refresh request so that the New Tab page can be correctly displayed. See the Embedded Search API for more details. Your search engine may also record your interactions with the New Tab page.

The New Tab page content may be designed by your default search provider. Suggested websites are embedded by Chrome into the New Tab page in a way that does not expose them to your default search provider.

This information about the New Tab page may not apply if you've installed an extension that overrides the New Tab page.

Tap to Search

If you've enabled "Tap to Search" on Chrome Mobile you can search for terms by tapping them.

When you tap a word, the word, the surrounding text, and the home country of your device's SIM card are sent to Google to identify recommended search terms (for example, tapping on "Michael" on a site about Michael Jackson might lead to a suggested search for "Michael Jackson"). The tapped word is logged in accordance with standard Google logging policies, and the surrounding text and home country are logged only when the page is already in Google's search index. If you sync your browsing history, the URL of the page is also sent and logged, and is used to improve your query suggestions.

When Google returns a search suggestion, a card "peeks through" at the bottom of the screen, showing the suggested search term. Opening this card is considered a regular search and navigation on Google, so standard logging policies apply.

Long-pressing on a word opens a peeking card with the selected word, except on recent versions of Android Oreo and higher which activates Smart Text Selection instead. No communication with Google occurs until the card is opened, and no surrounding text is sent. Saying "Ok Google" after long-pressing on a word provides the word and its surrounding text as context for the Google Assistant.

Tap to Search is enabled in a limited mode by default: potentially privacy-sensitive data, such as the URL and surrounding text, is not sent for HTTPS pages. Tap to Search can be fully enabled and disabled in the card or in the Chrome privacy settings.

More like this

If you have chosen to sync your browsing history, Chrome may provide contextually relevant content recommendations on certain pages via a "More like this" button on the top toolbar and the suggestions will be shown from a bottom sheet.

In order to provide these suggestions, the URL of the page that you're currently viewing, along with your language or locale information and IP address is sent to Google. Suggestions are only fetched for HTTP and HTTPS pages, not pages with other schemas like file: or ftp:. Selected suggestions are logged in accordance with standard Google logging policies.

Suggestions are not available on all webpages. When there are suggestions, the "More like this" button will appear on the top toolbar.

Safe Browsing protection

Google Chrome includes an optional feature called "Safe Browsing" to help protect you against phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. You can find more information at safebrowsing.google.com about how Safe Browsing protects you in Chrome and other Google products. Safe Browsing is designed specifically to protect your privacy and is also used by other popular browsers. This feature is not available on the iOS version of Chrome.

You can find settings for Safe Browsing in the "Sync and Google services" section of Chrome's settings on desktop and in the "Privacy" section of Chrome's settings on mobile. When Safe Browsing is enabled in Chrome, Chrome contacts

Google's servers periodically to download the most recent Safe Browsing list of unsafe extensions and sites, including phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. The most recent copy of this list is stored locally on your system. Chrome checks the URL of each site you visit or file you download against this local list. If you navigate to a URL that appears on the list, Chrome sends a partial URL fingerprint (the first 32 bits of a SHA-256 hash of the URL) to Google for verification that the URL is indeed dangerous. Chrome also sends a partial URL fingerprint when a site requests a potentially dangerous permission, so that Google can protect you if the site is malicious. Google cannot determine the actual URL from this information.

In addition to the URL check described above, Chrome also conducts client-side checks. If a website looks suspicious, Chrome sends a subset of likely phishing and social engineering terms found on the page to Google, in order to determine whether the website should be considered malicious. Chrome can also help protect you from phishing if you type one of your previously saved passwords into an uncommon site. In this case Chrome sends the URL and referrers of the page to Google to see if the page might be trying to steal your password.

If you encounter a website that is on Chrome's Safe Browsing list, you may see a warning like the one shown below.



You can [visit our malware warning test page](#) or [social engineering warning test page](#) to see the above example in action. For more information about the warning pages, see [Manage warnings about unsafe sites](#).

You can also opt in to reporting additional [data relevant to security](#) to help improve Safe Browsing and security on the Internet. On desktop, you can opt in by turning on the "Help improve Safe Browsing" setting in the "Sync and Google services" section of Chrome's settings. On mobile, this setting is in the "Privacy" section of Chrome's settings. You can also opt in from the warning page shown above. If you opt in, Chrome will send an incident report to Google every time you receive a warning, visit a suspicious page, and on a very small fraction of sites where Chrome thinks there could be threats, to help Safe Browsing learn about the new threats you may be encountering. The reports are sent to Google over an encrypted channel and can include URLs, headers, and snippets of content from the page and they never include data from browsing you do in Incognito mode. If Chrome discovers unwanted or malicious software on your machine, the reports may also include details about malicious files and registry entries. This data is used only to improve Safe Browsing and to improve security on the Internet. For example, Chrome reports some [SSL certificate](#) chains to Google to help improve the accuracy of Chrome's SSL warnings..

Please be aware that if you disable the Safe Browsing feature, Chrome will no longer be able to protect you from websites that try to steal your information or install harmful software. We don't recommend turning it off.

If you are a webmaster, developer, or network admin, you can find more relevant information about Safe Browsing on [this page](#).

Safe Browsing also protects you from abusive extensions and malicious software. At start up of Chrome, Safe Browsing scans extensions installed in your browser against the Safe Browsing list. If an extension on the list is found, Chrome will temporarily disable the extension, offer you relevant information and provide an option for you to remove the extension or re-enable it. Chrome also sends the particular extension ID to Safe Browsing. If you attempt to download a file on Chrome's Safe Browsing list, you'll see a warning like this one:



To warn you about potentially dangerous files, like the picture shown above, Chrome checks the URL of potentially dangerous file types you download against a list of URLs that have been verified. Potentially dangerous file types includes both executables and commonly-abused document types. This list is stored locally on your computer and updated regularly. Chrome does not send information to Google for files you download from URLs in this list, or if the file is signed by a verified publisher. For all other unverified potentially dangerous file downloads, Chrome sends Google the information needed to help determine whether the download is harmful, including some or all of the following: information about the full URL of the site or file download, all related referrers and redirects, code signing certificates, file hashes, and file header information. Chrome may then show a warning like the one pictured above.

Chrome helps protect you against password phishing by checking with Google when you enter your password on an uncommon page. Chrome keeps a local list of popular websites that Safe Browsing found to be safe. If Chrome detects that you have entered your Google account password or one of your passwords stored in Chrome's password manager on a website that's not on the list, it sends a request to Safe Browsing to gather the reputation of that website. The verdict received from Safe Browsing is usually cached on your device for 1 week.

If the reused password is your Google account password and the verdict for the website is that it is phishing, Chrome will suggest that you change your Google account password to avoid losing access to your account. Additionally, if you sync your browsing history without a sync passphrase, Chrome sends another request to tell Google that your password was likely phished, to make hijacking of your Google account by an adversary more difficult. The information sent in this request includes the ID of the synced browsing history entry to identify the URL where the phishing attempt happened, and the verdict received from Safe Browsing.

If you've opted into "Help improve Safe Browsing", Chrome also sends a request to Safe Browsing each time you start to enter a password on a page that isn't in Chrome's local list. In addition, the request Chrome sends to Safe Browsing to determine the reputation of the website on which you reuse your password includes the list of websites for which you saved this password in Chrome's password manager (but not the password itself).

If Chrome detects that your settings have been tampered with, Chrome reports the URL of the last downloaded potentially dangerous file, and information about the nature of the possible tampering, to the Safe Browsing service.

For some downloads, Chrome may ask you to opt in to reporting to Google Safe Browsing some data relevant to security, in order to improve the quality of download protection. Once you've opted in, some downloaded files that are suspicious will be sent to Google for investigation each time they are encountered. You can change this opt-in setting at any time in the Chrome settings.

Chrome asks your permission before using certain web features (APIs) that might have associated risks. To improve the safety and utility of Chrome permissions, Chrome may anonymously report the domains on which you grant, reject and revoke permissions or ignore or dismiss permission prompts. This happens only if you are a Safe Browsing user and have activated syncing your browsing history and settings with Google without a custom passphrase.

For all Safe Browsing requests and reports, Google logs the transferred data in its raw form and retains this data for up to 30 days. Google collects standard log information for Safe Browsing requests, including an IP address and one or more cookies. After at most 30 days, Safe Browsing deletes the raw logs, storing only calculated data in an anonymized form that does not include your IP addresses or cookies. Additionally, Safe Browsing requests won't be associated with your Google Account. They are, however, tied to the other Safe Browsing requests made from the same device.

Unwanted software protection

The Windows version of Chrome is able to detect and remove certain types of software that violate [Google's Unwanted Software Policy](#). If left in your system, this software may perform unwanted actions, such as changing your Chrome settings without your approval. Chrome periodically scans your device to detect potentially unwanted software. In addition, if you have opted in to automatically report details of possible security incidents to Google, Chrome will report information about unwanted software, including relevant file metadata and system settings linked to the unwanted software found on your computer.

If you perform an unwanted software check on your computer from the Settings page, Chrome reports information about unwanted software and your system. System information includes metadata about programs installed or running on your system that could be associated with harmful software, such as: services and processes, scheduled tasks, system registry values commonly used by malicious software, command-line arguments of Chrome shortcuts, Windows proxy settings, and software modules loaded into Chrome or the network stack. You can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the scan.

If unwanted software is detected, Chrome will offer you an option to clean it up by using the Chrome Cleanup Tool. This will [quarantine](#) detected malicious files, delete harmful extensions and registry keys, and [reset](#) your settings. The Chrome Cleanup Tool also reports information about unwanted software and your system to Google, and again you can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the cleanup.

This data is used for the purpose of improving Google's ability to detect unwanted software and offer better protection to Chrome users. It is used in accordance with Google's [Privacy Policy](#) and is stored for up to 14 days, after which only aggregated statistics are retained.

Navigation error tips

Google Chrome can show tips to help guide you to the page you were trying to reach in cases where the web address cannot be found, a connection cannot be made, the server returns a very short (under 512 byte) error message, or you've navigated to a parked domain.

Google Chrome will first check the address against a locally-stored list of suspected parked domains. If there is a match, Chrome sends a partial fingerprint (a hash prefix) of the URL to Google for verification that the domain is indeed parked. This uses the same methodology as the Safe Browsing service (see the "Safe Browsing protection" section, above).

In the case of other navigation errors, the URL of the web page you're trying to reach is stripped of all GET parameters, and then sent to Google in order to retrieve navigation tips. This information is logged and anonymized in the same manner as [Google web searches](#). The logs are used to ensure and improve the quality of the feature.

Additionally, to provide you with more informative error messages when a domain name cannot be found, Chrome will investigate the underlying cause by attempting to resolve "google.com" using both [Google Public DNS](#) and the default DNS service configured for your system.

In the event that Chrome detects SSL connection timeouts, certificate errors, or other network issues that might be caused by a captive portal (a hotel's WiFi network, for instance), Chrome will make a cookieless request to https://www.gstatic.com/generate_204 and check the response code. If that request is redirected, Chrome will open the redirect target in a new tab on the assumption that it's a login page. Requests to the captive portal detection page are not logged.

You can [disable navigation error tips](#) by unchecking the box in the "Sync and Google services" section of Chrome's settings on desktop and in the "Privacy" section of Chrome's settings on mobile.

Offline Indicator

On Android versions Lollipop and older, when Chrome detects a network change, it sends a cookieless request to http://connectivitycheck.gstatic.com/generate_204 or http://clients4.google.com/generate_204 to determine whether you're offline and display an offline indicator.

Desktop versions of Chrome and the Google Chrome Apps Launcher use Google Update to keep you up to date with the latest and most secure versions of software. In order to provide greater transparency and to make the technology available to other applications, the Google Update technology is open source.

Google Update requests include information necessary for the update process, such as the version of Chrome, its release channel, basic hardware information, and update errors that have been encountered. The update requests also send Google information that helps us understand how many people are using Google Chrome and the Chrome Apps Launcher – specifically, whether the software was used in the last day, the number of days since the last time it was used, the total number of days it has been installed, and the number of active profiles. Google Update also periodically sends a non-unique four-letter tag that contains information about how you obtained Google Chrome. This tag is not personally identifiable, does not encode any information about when you obtained Google Chrome, and is the same as everyone who obtained Google Chrome the same way.

Because Chrome OS updates the entire OS stack, Google Update on Chrome OS also sends the current Chrome OS version and hardware model information to Google in order to ensure that the correct software updates and hardware manufacturer customizations such as apps, wallpaper, and help articles are delivered. This information is not personally identifiable, and is common to all users of Chrome OS on the same revision of device.

Unlike the desktop versions of Chrome, the delivery and management of updates for mobile versions of Chrome are managed through the app stores for Android and iOS. Mobile versions of Chrome utilize the servers described above for counting active installations.

Chrome extensions and applications that you've installed are kept up to date with a similar system used for updating desktop versions of Chrome. These update requests include similar information (such as the application ID, when the application was last used, and how long it's been installed). We use these requests to determine the aggregate popularity and usage of applications and extensions. If you are using an extension or application restricted to a certain audience, authentication tokens are sent with the update requests for these add-ons. For security reasons, Chrome also occasionally sends a cookieless request to the Chrome Web Store, in order to verify that installed extensions and applications that claim to be from the store are genuine.

In order to keep updates as small as possible, Google Chrome is internally split into a variety of components, each of which can be updated independently. Each component is uniquely identified via an ID that is shared among all Google Chrome installations (e.g., "fmeadaodfnidclnjhlkdgjkolmhmfmofk"). An update request for a component contains this ID, the hash of the previous download (called a "fingerprint"), and the component's version. Because every installation has the same ID, and downloads of the same component have the same fingerprint, none of this information is personally identifiable.

If you install web apps on an Android device, a Google server is responsible for creating a native Android package that can be verified for authenticity by Chrome. When Chrome is updated or notices that the web app's manifest has changed, Chrome asks the server for a new version of the Android package in a cookieless request. If the information needed to create the native Android package cannot be acquired by the server (e.g., because the information is behind a corporate firewall), Chrome sends it to Google and an Android package is created that is unique to you. It contains a unique and random identifier that is not tied to your identity.

Chrome may also download and run a binary executable (e.g., as part of the software update or to improve Safe Browsing protection). These executables are cryptographically signed and verified before execution. Chrome may download further static resources like dictionaries on demand to reduce the size of the installer.

On Windows and OS X versions of Chrome, the recovery component tries to repair Google Update when it's broken. After the relevant binary is executed, Google Update uploads statistics on the actions that were performed. These statistics contain no personally identifiable information.

Network time

On desktop platforms, Chrome uses network time to verify SSL certificates, which are valid only for a specified time. At random intervals or when Chrome encounters an expired SSL certificate, Chrome may send requests to Google to obtain the time from a trusted source. These requests are more frequent if Chrome believes the system clock is inaccurate. These requests contain no cookies and are not logged on the server.

Counting installations

In order to measure the success rate of Google Chrome downloads and installations of the Windows version of Google Chrome, a randomly-generated token is included with Google Chrome's installer. This token is sent to Google during the installation process to confirm the success of that particular installation. A new token is generated for every install. It is not associated with any personal information, and is deleted once Google Chrome runs and checks for updates the first time.

For Chrome to know how many active installations it has, the mobile version of Chrome sends a ping to Google with a salted hash of a device identifier on an ongoing basis. The desktop version of Chrome does not send any stable identifier to count active installations. Instead an anonymous message to Google with a timestamp of the last ping is used to infer number of active installations.

Measuring effectiveness of a promotion

Chrome utilizes two measurements to understand how effective a promotional campaign has been: how many Chrome installations are acquired through a promotional campaign, and how much Chrome usage and traffic to Google is driven by a campaign.

To measure installations or reactivations of Chrome through a campaign, Chrome will send a token or an identifier unique to your device to Google at the first launch of Chrome, as well as the first search using Google. On desktop versions of Chrome, a token unique to your device is generated. The same token will be sent if Chrome is later reinstalled at first launch and at first use of the Omnibox after reinstallation or reactivation. Rather than storing the token on the computer, it is generated when necessary by using built-in system information that is scrambled in an irreversible manner. On iOS, Chrome uses the IDFA for counting installations acquired by a campaign, and it can be reset in iOS settings.

To measure searches and Chrome usage driven by a particular campaign, Chrome inserts a promotional tag, not unique to you or your device, in the searches you perform on Google. This non-unique tag contains information about how Chrome was obtained, the week when Chrome was installed, and the week when the first search was performed. For desktop versions of Chrome, Chrome generates a promotional tag, if the promotional installation token described in the previous paragraph indicates that Chrome has been installed or reactivated by a campaign on a device which has not been associated with any campaign yet. For Chrome on Mobile, a promotional tag is always sent regardless of the source of installations.

The promotional tag is generated using a software library called "RLZ" and looks similar to "1T4ADBR_enUS236US239". The RLZ library was fully open-sourced in June 2010. For more information, please see the In the Open, for RLZ post on the Chromium blog and the article "How To Read An RLZ String". On Android, this promotional tag can also be a readable string like "android-hms-tmobile-us" instead of an RLZ string, and is not unique to either you or your device.

This non-unique promotional tag is included when performing searches via Google (the tag appears as a parameter beginning with "rlz=" when triggered from the Omnibox, or as an "x-rlz-string" HTTP header). We use this information to measure the searches and Chrome usage driven by a particular promotion.



If usage statistics and crash reports are enabled, the RLZ string is sent along with the report. This allows us to improve Chrome based on variations that are limited to specific geographic regions.

For the desktop version of Chrome, you can opt-out of sending this data to Google by uninstalling Chrome, and installing a version downloaded directly from www.google.com/chrome. To opt-out of sending the RLZ string in Chrome OS, press Ctrl + Alt + T to open the crosh shell, type rlz disable followed by the enter key, and then reboot your device.

Usage statistics and crash reports

Chrome has a feature to automatically send usage statistics and crash reports to Google in order to help improve Chrome's feature set and stability.



Usage statistics contain information such as system information, preferences, user interface feature usage, responsiveness, and memory usage. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs or personal information depending on what was happening at the time of the crash. This feature is enabled by default for Chrome installations of version 54 or later. You can control the feature in the "Sync and Google services" section of Chrome's settings on desktop and in the "Privacy" section of Chrome's settings on mobile. These statistics do not include any personal information.

When this feature is enabled, Google Chrome stores a randomly generated unique token on your device, which is sent to Google along with your usage statistics and crash reports. The token does not contain any personal information and is used to de-duplicate reports and maintain accuracy in statistics. This token is deleted when the feature is disabled and a new token is regenerated when the feature is enabled again.

Along with usage statistics and crash reports, Chrome also reports anonymous, randomized data that is constructed in a manner which is not linked to the unique token, and which ensures that no information can be inferred about any particular user's activity. This data collection mechanism is summarized on the Google research blog, and full technical details have been published in a technical report and presented at the 2014 ACM Computer and Communications Security conference.

Chrome will also anonymously report to Google if requests to websites operated by Google fail or succeed in order to detect and fix problems quickly.

If you are also syncing your browsing history without a sync passphrase on mobile or have also turned on "Make searches and browsing better (Sends URLs of pages you visit to Google)" in the "Sync and Google services" section of settings on desktop, Chrome usage statistics include information about the web pages you visit and your usage of them. The information will also include the URLs and statistics related to downloaded files. If you sync extensions, these statistics will also include information about the extensions that have been installed from Chrome Web Store. The URLs and statistics are sent along with a unique device identifier that can be reset by turning off history sync on mobile or by turning off "Make searches and browsing better" on desktop, or by turning off usage statistics and crash reports on any platform. The usage statistics are not tied to your Google account. Google only stores usage statistics associated with published extensions, and URLs that are known by Google's web crawlers. We use this information to improve our

products and services, for example, by identifying web pages which load slowly, this gives us insight into how to best improve overall Chrome performance. We also make some statistics available externally, through efforts like the [Chrome User Experience Report](#). Externally published reports are conducted in highly aggregated manner to not reveal individual user's identity.

On iOS, if you are syncing your browsing history without a sync passphrase, Chrome reports usage for certain URLs that other Google apps could open. For example, when you tap on an email address, Chrome presents a dialog that allows you to choose between opening with Google Gmail or other mail apps installed on your device. The usage information also includes which apps were presented to you, which one was selected, and if a Google app was installed. Chrome does not log the actual URL tapped. If you are signed in, this usage is tied to your Google account. If you are signed out, the information is sent to Google with a unique device identifier that can be regenerated by resetting the Google Usage ID found in Chrome settings. The raw reports are deleted within 60 days, after which only the aggregated statistics remain.

Google Surveys in Chrome

When you have "send usage statistics" enabled, you may be randomly selected to participate in surveys to evaluate consumer satisfaction with Chrome features. If you are selected, Chrome on Android requests a survey from Google for you. If a survey is available, Chrome then asks you to answer the survey and submit the responses to Google.

The survey also records basic metrics about your actions, such as time spent looking at the survey and elements that the user clicked. These metrics are sent to Google even if you do not fully complete the survey.

To ensure that surveys are spread evenly across users and not repeatedly served to a single user, the feature stores a randomly generated unique token on the device. This token is used solely for the survey requests and does not contain any personal information. If you disable sending usage statistics, the token will be cleared.

Suggestions for spelling errors

Desktop versions of Chrome can provide smarter spell-checking by sending text you type into the browser to Google's servers, allowing you to apply the same spell-checking technology that's used by Google products like Docs. If this feature is enabled, Chrome sends the entire contents of text fields as you type in them to Google, along with the browser's default language. Google returns a list of suggested spellings that are displayed in the context menu. Cookies are not sent along with these requests. Requests are logged temporarily and anonymously for debugging and quality improvement purposes.

This feature is disabled by default; to turn it on, click "Ask Google for suggestions" in the context menu that appears when you right-click on a misspelled word. You can also turn this feature on or off with the "Enhanced spell check" checkbox in the "Sync and Google services" section of Chrome settings. When the feature is turned off, spelling suggestions are generated locally without sending data to Google's servers.

Mobile versions of Chrome rely on the operating system to provide spell-checking.

Translate

Google Chrome's built-in translation feature helps you read more of the Web, regardless of the language of the web page. The feature is enabled by default.



Translation can be disabled at any time in Chrome's settings.

Language *detection* is done entirely using a client-side library, and does not involve any Google servers. For *translation*, the contents of a web page are only sent to Google if you explicitly decide to translate it by clicking "Translate" on the bar, or if you've previously chosen "Always translate" for a given language via the translate bar Options menu.

If you do choose to translate a web page, the text of that page is sent to [Google Translate](#) for translation. Your cookies are not sent along with that request and the request is sent over SSL. This communication with Google's translation service is covered by the [Google privacy policy](#).

If you've chosen to sync your Chrome history, statistics about the languages of pages you visit and about your interactions with the translation feature will be sent to Google to improve Chrome's understanding of the languages you speak and when Chrome should offer to translate text for you.

Sign In to Chrome and sync

You have the option to use the Chrome browser while signed in to your Google Account, with or without sync enabled.

On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. If you are signed in to Chrome, Chrome may offer to save your payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can turn off Chrome sign-in.

When you're signed-in and have enabled sync with your Google Account, your personal browsing data information is

saved in your Google Account so you may access it when you sign in and sync to Chrome on other computers and devices. Synced data can include bookmarks, saved passwords, open tabs, browsing history, extensions, addresses, phone numbers, payment methods, and more. In advanced sync settings, you can choose which types of data to synchronize with this device. By default, all syncable data types are enabled. You can turn sync on or off in the “People” section of Chrome settings.

If you have turned on sync and signed out of the account you are syncing to, sync will pause sending all syncable data to Google until you sign back in with the same account. Some sync data types (such as bookmarks and passwords) that are saved locally while sync is paused will automatically be synced to your account after you sign back in with the same account.

On mobile versions of Chrome, you can sign into or sign out of Chrome from Chrome settings. Signing into Chrome will also turn on sync. This can be done for any account that has already been added to the mobile device without authenticating again.

On both desktop and mobile, signing into Chrome keeps you signed into Google web services until you sign out of Chrome. On mobile, signing into Chrome will keep you signed in with all Google Accounts that have been added to the device. On desktop, it will keep you signed in with all Google Accounts that you added from a Google web service, unless you have set “Keep local data only until you quit your browser” in your [cookie settings](#).

On Android and desktop, Chrome signals to Google web services that you are signed into Chrome by attaching an X-Chrome-Connected and/or C-Chrome-ID-Consistency-Request header to any HTTPS requests to Google-owned domains. On iOS, the CHROME_CONNECTED cookie is used instead. This allows those Google web services to update their UI accordingly. If you are using a managed device, your system admin may disable the sign in feature or require that data be deleted when you disconnect your account.

Google uses your personal synchronized data to provide you a consistent browsing experience across your devices, and to customize features in Chrome. You can manage your synchronized history by going to [chrome://history](#) in your Chrome browser. If “Include history from Chrome and other apps in your Web & App Activity” is checked on the [Web & App Activity](#) controls page, Google also uses your synchronized browsing data to provide personalized Google products and services to you. You can change your preference any time, and manage individual [activities associated with your Google account](#).

The paragraph above describes the use of your personal browsing history. Google also uses aggregated and anonymized synchronized browsing data to improve other Google products and services. For example, we use this information to improve Google Search by helping to detect mobile friendly pages, pages which have stopped serving content, and downloads of malware.

If you would like to use Google's cloud to store and sync your Chrome data without allowing any personalized and aggregated use by Google as described in the previous paragraphs, you can choose to encrypt all of your synced data with a [sync passphrase](#). If you choose this option, it's important to note that Google won't have access to the sync passphrase you set; we won't be able to help you recover data if you forget the passphrase. Regardless of how you choose to encrypt your data, all data is always sent over secure SSL connections to Google's servers.

If you're signed into Chrome and are syncing passwords and/or other types of login credentials without a sync passphrase, these credentials are stored in your Google Account. Chrome may help you sign in with credentials you've saved in Android apps on websites that are associated with the respective apps. Likewise, credentials you've saved for websites can be used to help you sign into related Android apps. You can view the credentials you've saved in Chrome and Android by visiting [passwords.google.com](#) in any browser. If you've saved credentials for Android applications, Chrome periodically sends a cookieless request to Google to get an updated list of websites that are associated with those applications. To stop websites and Android apps from automatically signing in using credentials you previously saved, you can turn off Auto Sign-In on [passwords.google.com](#) or in Chrome settings under “Manage passwords”. For more details see [this article](#).

On mobile versions of Chrome, if you sync your browsing history without a sync passphrase and your browser's usage statistics and crash reports setting is also enabled, your usage statistics and crash reports will include statistics about the pages you visit. You can read more in the [Usage statistics and crash reports](#) section of this Whitepaper.

All data synchronized through Google's servers is subject to [Google's Privacy Policy](#). To get an overview of the Chrome data stored for your Google Account, go to the [Chrome section of Google Dashboard](#). That page also allows you to stop synchronization completely and delete all sync data from Google's servers.

Autofill and Password Management

Google Chrome has a [form autofill](#) feature that helps you fill out forms on the web more quickly. Autofill is enabled by default, but it can be turned off at any time in Chrome's settings.

If Autofill is enabled and you encounter a web page containing a form, Chrome sends some information about that form to Google. This information includes a hash of the web page's hostname, as well as form identifiers (such as field names), and the basic structure of the form. In response, Chrome receives a prediction of each field's data type (for example, “field X is a phone number, and field Y is a country”). This information helps Chrome match up your locally stored Autofill data with the fields of the form.

If Autofill is enabled when you *submit* a form, Chrome sends Google some information about the form along with the types of data you submitted. This information includes a hash of the web page's hostname, as well as form identifiers (such as field names), the basic structure of the form, and the observed data types for the fields (i.e., field X was a

You can manage your Autofill entries via [Chrome's settings](#), and you can edit or delete saved information at any time. Chrome will never store full credit card information (card number, cardholder name, and expiration date) without explicit confirmation. In order to prevent offering to save cards you have shown disinterest in saving, Chrome stores the last four digits of detected credit cards locally on the device. If you scan your credit card using a phone camera, the recognition is performed locally.

Chrome may help you sign in to websites with credentials you've saved to Chrome's password manager or Google Smart Lock by autofilling sign-in forms, by offering you an account picker, or by automatically signing you in. You can manage and delete your saved credentials in the "Forms and passwords" section of Chrome's settings. If you enable [password management](#), the same kind of data about forms as described above is sent to Google to interpret password forms correctly and enable Chrome to offer password generation that meets site-specific requirements.

Also, if you choose, you can bring your Autofill data with you to all your Chrome-enabled devices by [syncing it](#) as part of your browser settings (see the "Sign In to Chrome" section of this document). If you choose to sync Autofill information, field values are sent as described in "Sign In to Chrome"; otherwise, field values are not sent.

Payments

When you're signed into Chrome with your Google Account, Chrome may offer to save payment cards and related billing addresses into payment data under the same Google account, and include cards from your account among the autofill suggestions on payment web forms. Integration with Google Payments can be disabled via Chrome's Advanced sync settings. If integration with Google Payments is disabled, credit cards will be saved locally but will not be synced. If integration with Google Payments is enabled, Chrome may offer to autofill forms with credit card data stored in your Google Payments account. The cards from your Google Payments account not already saved locally are masked until you provide the correct CVV code. When providing your CVV code for verification, you can choose to store the credit card locally as part of your Chrome Autofill data. If you choose not to store the card locally, you will be prompted for your CVV code each time you use the card. If you use a card from Google Payments, Chrome will collect information about your computer and share it with Google Payments to prevent fraudulent use of your card.

To delete credit card information saved in Chrome, follow the "Add and edit credit cards" steps in [the Autofill article](#). When you delete a credit card that's also saved in your Google Payments account, you will be redirected to the Google Payments to complete the deletion. After your card has been deleted from your Google Payments account, Chrome will automatically remove that card from your Autofill suggestions.

To save a card locally on the device only, while still being signed in to Chrome with a Google Account, you can add a card from the "Add" button in the "Payment methods" section in Chrome settings. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can [turn off Chrome sign-in](#). If you have sync turned on, you can disable syncing payment methods and addresses to Google Pay under "Sync" in Chrome settings. You can also turn the Payments Autofill feature off altogether in [settings](#).

Chrome also supports the [PaymentRequest API](#) by allowing you to pay for purchases with credit cards from Autofill, Google Payments, and other payment apps already installed on your device. Google Payments and other payment apps are only available on an Android device. PaymentRequest allows the merchant to request the following information: full name, shipping address, billing address, phone number, email, credit card number, credit card expiration, CVV, and Google Payments credentials. Information is not shared with the merchant until you agree.

Geolocation

Google Chrome supports the [Geolocation API](#), which provides access to fine-grained user location information with your consent.

By default, Chrome will request your permission when a web page asks for your location information, and does not send any location information to the web page unless you explicitly consent.

Furthermore, whenever you are on a web page which is using your location information, Chrome will display a location icon on the right side of the omnibox. You can click on this icon in order to find out more information or manage location settings.



In [Chrome's settings](#), by clicking "Show advanced settings.", then clicking "Content Settings" and scrolling to the "Location" section, you can choose to allow all sites to receive your location information, have Chrome ask you every time (the default), or block all sites from receiving your location information. You can also configure exceptions for specific web sites.

In the Android version of Chrome, your default search engine automatically receives your location when you conduct a search. On the iOS version of Chrome, by default your location is sent to Google if you conduct a search from the omnibox. Read more about how your default search engine handles geolocation and how to manage your settings in the [Omnibox](#) section of the whitepaper.

If you do choose to share your location with a web site, Chrome will send local network information to Google (also used by other browsers such as Mozilla Firefox) in order to estimate your location. This local network information can include data about nearby Wi-Fi access points or cellular signal sites/towers (even if you're not using them), and your

For further reading on the privacy and user interface implications of the Geolocation API (as well as other HTML5 APIs), see "[Practical Privacy Concerns in a Real World Browser](#)" written by two Google Chrome team members.

Speech to text

Chrome supports the [Web Speech API](#), a mechanism for converting speech to text on a web page. It uses Google's servers to perform the conversion. Using the feature sends an audio recording to Google (audio data is not sent directly to the page itself), along with the domain of the website using the API, your default browser language and the language settings of the website. Cookies are not sent along with these requests.

Google Assistant "Ok Google"

The Google Assistant feature is integrated into some models of Chrome OS devices. If you opt in to the feature, Chrome OS listens for you to say "Ok Google" and sends the audio of the next thing you say, plus a few seconds before, to Google. Detection of the phrase "Ok Google" is performed locally on your computer, and the audio is only sent to Google after it detects "Ok Google". You can enable or disable this feature in Google Assistant Settings.

Enabling this feature in Chrome Settings will cause Chrome to listen whenever the screen is unlocked. On Chrome OS devices with a local audio processor, the device also listens when the device is asleep. On these devices, The Google Assistant feature only works if [Voice & Audio Activity](#) is enabled for your Google account. Chrome will prompt you to enable [Voice & Audio Activity](#) for the associated Google account if it is disabled.

Once the audio has been converted to text, a search with that text is submitted to Google. If you have used the "Ok Google" search before on a device but turned off Voice & Audio Activity later, your device is still capable of processing your voice and sending the audio to Google but the voice is deleted shortly.

You can determine your Chrome OS device's behavior by examining the text in the "Search and Assistant" section of settings.

Google Cloud Print

The [Google Cloud Print](#) feature allows you to print documents from your browser over the Internet. You do not need a direct connection between the machine that executes Chrome and your printer.

If you choose to print a web page via Cloud Print, Chrome will generate a PDF of this website and upload it over an encrypted network connection to Google's servers. If you choose to print other kinds of documents, they may be uploaded as raw documents to Google's servers.

A print job will be downloaded by either a Chrome browser ("Connector") or a Cloud Print capable printer that you selected when printing the website. In some cases the print job must be submitted to a third-party service to print (HP's ePrint, for example).

The print job is deleted from Google's servers when any of three criteria is met:

- You delete the print job
- The job has been printed and marked as printed by the printer/connector
- The job has been queued on Google's servers for 30 days

You can manage your printers and print jobs on the [Google Cloud Print website](#).

SSL certificate reporting

Chrome stores locally a list of expected SSL certificate information for a variety of high-value websites, in an effort to [prevent man-in-the-middle attacks](#). For Google websites and other websites that choose to opt in, Chrome will report a possible attack or misconfiguration. If the certificate provided by the web server doesn't match the expected signature, Chrome reports information about the SSL certificate chain to Google or to a report collection endpoint of the website's choosing. Chrome sends these reports only for certificate chains that use a [public root of trust](#).

You can enable this feature by opting in to report data relevant to security, as described in the [Safe Browsing section](#). While you are opted in, two kinds of reports may be sent to Google's security team. Each time you see an SSL error page, a report will be sent containing the SSL certificate chain, the server's hostname, the local time, and relevant details about the validation error and SSL error page type. Additionally, each time a mismatch between different certificate verifiers is detected, a report will be sent containing the certificate chain and the verification result.

Because Chrome sends these reports for all certificate chains, even those that chain to a private root of trust, these chains can contain personally identifiable information. You can opt out anytime by unchecking the box "Help Improve Safe Browsing" in the Privacy section of Chrome's advanced settings.

The SSL certificate reporting feature is not available on Chrome iOS.

Installed Applications and Extensions

Users can install external apps and extensions for the desktop versions of Chrome to add features to or customize their

Chrome browsers. Installing an application or extension from the Chrome Web Store directly or via an inline installation flow on a third-party site involves a request to the Chrome Web Store for details about the application. This request includes cookies, and if you're logged into Google when you install an application, that installation is recorded as part of your Google account. The store uses this information to recommend applications to you in the future, and in aggregate to evaluate application popularity and usage. As noted above, applications and extensions are updated via Google Update.

As they're more deeply integrated into Chrome, applications and extensions that you choose to install can request access to additional capabilities, enabling functionality that doesn't make sense on the web at large: background notifications or raw socket access, for instance. These additional permissions may change the way your data is collected and shared, as extensions and applications might have access to data regarding the websites you visit, and might be capable of monitoring or modifying your interactions with the web. When installing an application or extension, Chrome may first warn you about certain capabilities. Please do take the time to read and evaluate this warning before proceeding with the installation. Note also that interactions with and data collected by these third-party applications and extensions are governed by their own privacy policies, not Google's privacy policy.

Push messaging

Your device may receive push messages from the backend servers of apps and extensions installed in Chrome, websites that you grant the "notification" permission to, and your default search engine. Disabling push messages from your default search engine is done in the same way as disabling push messages from any site, by visiting the "Notifications" section of "Site settings".

Push message data is sent over a secure channel from the developer through Google's infrastructure to Chrome on your device, which can wake up apps, extensions, and websites (including your default search engine) to deliver the message. The developer may end-to-end encrypt the message data, or may send it in a form such that Google servers process it as plain text. Google servers retain up to 4 weeks' worth of messages to ensure delivery to users even if their devices are offline at the time of the initial pushing.

If the notification permission is set to "granted" for any website (including the default search engine), or you have an app or extension installed that uses push messaging, then Chrome provides the app's, extension's, or website's server with one or more registration tokens that can be used to send messages to the entity (app, extension, or website). Websites you visit in Incognito mode are not allowed to send you push messages and therefore cannot get a registration token.

When you uninstall an app or extension, revoke the notification permission for a website, or clear cookies for a permitted website, its registration token is revoked and will not be reused, even if the same app or extension is re-installed or the same website is re-visited. Registration tokens used by Chrome components such as Sync are revoked once they are no longer in use (for example, when the user disables Sync). When a registration token is revoked, the associated entity on your device stops receiving messages sent from its developer's server.

The registration tokens that are passed to entities contain an encrypted device ID, which is used for routing the messages. Google can decrypt the device ID, but other entities cannot, and the encryption is designed so that two registration tokens for the same device ID cannot be correlated. On desktop versions of Chrome, the device ID is reset when the Chrome profile is removed (via the "People" section in Chrome's Settings), or when neither Chrome Sync nor any of the entities requires it for push messaging. On Android, the lifetime of the device ID is governed by the operating system and is independent of Chrome. Any messages routed to registration tokens containing a revoked device ID will not be delivered.

Chrome custom tabs

On Android devices, an app developer may use a Custom Tab to show web content when you click on a URL from their app. A Custom Tab may look different from a regular Chrome tab, for example it may have app-specified visual style, and the absence of an editable URL bar. Despite the different visual style a Custom Tab may have, the data sent and received in the Custom Tab, such as cookies, saved passwords and browsing history function the same way they do in a normal Chrome tab. The Custom Tab is an app-customized view using the same underlying user profile.

With Chrome Custom Tabs, an Android app developer may also specify custom actions in the Chrome toolbar and overflow menu that are relevant to their app, for example, "share", "save page", "copy URL". If you tap on such a button, the address of the current website is shared with the application.

An application can request Chrome to pre-render a given URL in the background. This allows Chrome to show you a pre-loaded site instantly when you open it from the app. At the same time it allows an application to set cookies in your browser in the background. To disable pre-rendering, you can uncheck "Prefetch page resources" in the privacy settings.

Trusted Web Activities are a form of Chrome Custom Tab where the top bar is not present, allowing web browsing with no browser UI but with access to the cookie jar. They can only be used to view web content on an origin that the client app can prove that it owns using Digital Asset Links. If the user navigates off this origin the the top bar reappears.

When the client app is uninstalled or has its data cleared through Android Settings, Chrome will allow the user to clear data for the linked origin.

Continue where you left off

If you have selected the option to “Continue where you left off” in settings on desktop versions of Chrome, when you open Chrome, it attempts to bring you right back to the way things were when the browser was closed. Chrome reloads the tabs you had open and persists session information to get you up and running as quickly as possible. This feature effectively extends a browsing session across restarts. In this mode, session cookies are no longer deleted when the browser closes; instead, they remain available on restart to keep you logged into your favorite sites.

On desktop versions of Chrome, this feature can be enabled or disabled in Chrome settings. On Chrome OS, it is enabled by default.

On OS X, when you restart your device, a checkbox in the OS confirmation dialog asks you whether you want to re-open applications and windows after restart. If you check this box, Chrome restores tabs and windows, as well as the session cookies, even if you have disabled “Continue where you left off” on Chrome.

On mobile versions of Chrome, this feature is always enabled without a setting.

Chrome Variations

We want to build features that users want, so a subset of users may get a sneak peek at new functionality being tested before it’s launched to the world at large. A list of field trials that are currently active on your installation of Chrome will be included in all requests sent to Google. This Chrome-Variations header (X-Client-Data) will not contain any personally identifiable information, and will only describe the state of the installation of Chrome itself, including active variations, as well as server-side experiments that may affect the installation.

The variations active for a given installation are determined by a seed number which is randomly selected on first run. If usage statistics and crash reports are disabled, this number is chosen between 0 and 7999 (13 bits of entropy). If you would like to reset your variations seed, run Chrome with the command line flag “--reset-variation-state”. Experiments may be further limited by country (determined by your IP address), operating system, Chrome version and other parameters.

Do Not Track

If you enable the “Do Not Track” preference in Chrome’s settings, Chrome will send a DNT:1 HTTP header with your outgoing HTTP, HTTPS and SPDY browsing traffic (Chrome cannot, however, guarantee that NPAPI plugins also send the header.) The header will not be sent with system traffic such as the geolocation, metrics or device management services.

The effect of Do Not Track depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example, to improve security; to provide content, services, ads and recommendations on their websites; and to generate reporting statistics.

Chrome on iOS now uses WKWebView to provide a more stable and faster browser. As a result of this move, the Do Not Track preference is no longer available due to iOS constraints. If Apple makes changes to allow this feature, Chrome will make Do Not Track available again in iOS.

Plugins

Chrome ships with an Adobe Flash Player implementation that is based on the Pepper API. Flash and other Pepper-based plugins may ask you for “Access to your computer”. If you grant this permission, the plugin is granted unsandboxed access. This allows content providers to offer you access to DRM protected content like videos or music but may have security and privacy implications, so consider carefully whether you trust a plugin or website with this privilege.

Media licenses

Some websites encrypt media to protect against unauthorized access and copying. When users play media from these sites, they typically log into the site, which authenticates the user, and then digital rights management negotiates a key exchange for the decryption and playback of the media.

For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. The implementation of that API is tightly coupled with the browser to protect user privacy and security, through Content Decryption Modules (CDM), which are provided by digital rights management solutions such as Google Widevine or Microsoft PlayReady.

When a user asks Chrome to play encrypted HTML5 media (for example, watching a movie on Google Play Movies), Chrome will generate a request for a license to decrypt that media. This license request contains an automatically generated request ID, which is created by the Content Decryption Module, as well as proof that the CDM is legitimate. After generation, the license request is typically sent to a license server managed by either the content website or Google. Neither the license request, the proof, nor the request ID include any personally identifying information. After being sent, the license request is not stored locally on the user’s device.

As part of the license request, Chrome also generates a unique session ID which does not contain personally identifying information. This session ID is sent to the license server, and when the server returns a license the session ID is used to decrypt the media. The session ID may be stored locally even after the site has been closed. The license may also be stored locally for offline consumption of protected content. Session ID and licenses may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected.

When returning a license, the site license server may include a client ID generated by the site. This client ID is unique to the user and the site, it is not shared between sites. If provided, the client ID is stored locally and included by Chrome in subsequent license requests to that site. The client ID may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected.

On some platforms, the website may additionally request verification that the device is eligible to play specific types of protected content; on Chrome OS, this is known as [Verified Access](#)). In this case, Google creates a certificate using a unique hardware identifier for the device. This hardware ID identifies the device, but does not identify the user. If the user agrees, Google receives the hardware ID and generates a certificate verifying the device for the requested site. The certificate does not include the hardware ID or any other information that could permanently identify the device. Certificates are stored locally similar to other cached browsing data, and may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected.

Some sites use Flash instead of HTML5. If a website you visit chooses to use Adobe Flash Access DRM protection, Chrome for Windows and Chrome OS will give Adobe Flash access to a device identifier. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with “Cookies and other site data” selected.

In order to give you access to licensed music, the [Google Play Music app](#) can retrieve a device identifier that is derived from your hard drive partitions or, on a Chrome OS or Linux installation, from a unique file on your disk. This identifier can be reset by reinstalling your operating system.

Cloud policy

When you sign into a Chrome OS device, Chrome on Android, or a desktop Chrome profile with an account associated with a Google Apps domain, Chrome checks whether the domain has configured enterprise policies. If so, the Chrome OS user session or Chrome profile is assigned a unique ID, and registered as belonging to that domain. Any configured policies are applied to the profile. In order to revoke the registration, you'll need to remove the Chrome OS user profile, sign out of Chrome on Android, or remove the desktop profile.

Additionally, Chrome OS devices can be enrolled to a Google Apps domain by a domain admin. This will enforce enterprise policies for the entire device, such as providing shared network configurations and restricting access to developer mode. When a Chrome OS device is enrolled to a domain, then a unique device ID is registered to the device. In order to revoke the registration, the admin will need to wipe the entire Chrome OS device.

Registered profiles and devices check for policy changes periodically (every 3 hours by default). In some cases, the server pushes policy changes to the client without waiting for Chrome's periodic check. Unregistered profiles check whether a policy has been turned on for their domain each time Chrome starts up.

The [policy list](#) contains details about the types of configurations that are available via Cloud Policy.

Data Saver

If you enable Data Saver, Chrome will send your traffic through Google's optimizing proxy servers. This option reduces the amount of data downloaded and speeds up your page loads.

Most of the time, only your HTTP traffic is transparently proxied, and you won't notice any changes to the page. However, if Chrome anticipates the page will load especially slowly, both HTTP and HTTPS pages will be optimized to load only the essential content. For HTTPS origins, the transcoded pages are served from a Google-owned domain instead of being transparently proxied. Because these pages are served from a Google-owned domain instead of the original domain, Chrome will not send any origin-scoped information (e.g., cookies or data from local storage) for the original domain to Google, and Google cannot set any origin-scoped information for the original domain in Chrome. Pages loaded in Incognito are never proxied or optimized by Data Saver.

Request URLs are logged, but Cookie and If-None-Match headers are stripped from the logs (and cookies are never seen in the case of HTTPS pages). Additionally, the content of proxied pages is cached but not logged. The logs are not associated with your Google Account, and the entire log entry is removed within 14 days. These logs are also governed by standard Google search logging policies.

Google uses the logged and cached data to improve both Data Saver and Safe Browsing; for example, more effective optimizations can be uncovered by analyzing timing data for pages loaded through the proxy service, and malware can be detected more rapidly by analyzing response data in realtime.

Your IP address is forwarded to the origin HTTP server via an X-Forwarded-For header, in accordance with the HTTP standard. The Data Saver service is a transparent proxy, *not* an anonymization service.

By default, the connection between the browser and the Data Saver proxy is over an encrypted channel. However, a network administrator can [disable](#) the use of an encrypted channel to Data Saver.

Using Chrome with a kid's Google Account

Chrome for Android offers features to be used when signed in with a [kid's Google Account](#) and automatically signs in a kid's account if they've signed into the Android device. Chrome uses the [Sync feature](#) to sync settings configured by parents to the kid's account. You can read about how Sync data is used in the [Sign in](#) section of this Whitepaper.

The collection and use of Chrome data in association with a kid's Google Account are governed by the [Google Family](#)

In order for the configured settings to apply to a kid's account, Chrome does not support the following features for a kid's Google Account: signing out of Chrome, [Incognito mode](#), and deleting browsing history from within Chrome. Browsing history can still be removed in the [Chrome section of the Google Dashboard](#).

By default, first party cookie blocking is disabled when Chrome is signed in with a kid's account. Parents can go to [chrome.google.com/manage/family](#) to allow their kids to block first party cookies. However, blocking cookies signs kids out of Google web products such as Google Search or YouTube and therefore prevents these products from providing any features designed for kids' Google Accounts.

When Chrome is used with a kid's Google Account, information about the kid's requests to access blocked content is sent to Google and made visible to the kid's parent(s) on [chrome.google.com/manage/family](#) and in the [Google Family Link app](#). If the kid's browsing mode is set to "Try to block mature sites", Chrome will send a request to the Google [SafeSearch service](#) for each navigation in order to block access to sites that have been classified as containing mature content.

Incognito and Guest Mode

Incognito mode in Chrome is a temporary browsing mode. It ensures that you don't leave browsing history and cookies on your computer. The browsing history and cookies are deleted only once you have closed the last incognito window. Incognito mode cannot make you invisible on the internet. Websites that you navigate to may record your visits. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Browsing as a Guest in Chrome allows you to use somebody else's computer without modifying their profile. For example, no bookmarks or passwords get stored on their computer. Note that Guest mode does not protect you for example, if the computer you are using is infected by a keylogger that records what you type.

iOS 8 and Mac OS X Yosemite Handoff Support

While browsing in a standard (i.e. non-Incognito) session, Chrome will share your current URL with iOS 8+ to support the Handoff feature that was added in OS X Yosemite. This information is only sent to Apple devices that are paired with your iOS device, and the data is encrypted in transit.

More information is available at [Apple Support](#), [Apple Developers](#), and in the [Apple iOS Security Guide](#). Chrome support for this feature can be disabled in Chrome settings.

Security Key

A FIDO U2F Security Key provides a non-phishable credential which can be used to authenticate a user. This mitigates the risk of various kinds of man-in-the-middle attacks in which websites try to steal your password and use it later.

To prevent abuse, a website is required to be delivered over a secure connection (HTTPS), and to register the security key before it can be used for identification. Once a website is registered with a specific security key, that security key will provide a persistent identifier, regardless of which computer it is plugged into, or whether you're in incognito or guest mode, but you must physically interact with the security key to give a website access to an identifier (by, for example, touching it, or plugging it in).

Physical Web

The Physical Web lets you see a list of URLs being broadcast by objects in the environment around you. Google Chrome looks for Physical Web devices with Bluetooth Low Energy beacons that are broadcasting URLs using the Eddystone protocol. Bluetooth signals can be received from 90 feet away or more, depending on signal strength and the user's environment (although the range is often much shorter, due to obstacles and signal noise). If the Physical Web feature is enabled, Chrome sends detected URLs to Google's Physical Web Service (PWS) via a cookieless HTTPS request. For each URL, the PWS obtains the title of the web page, filters out unsafe results, and returns a ranking based on non-personalized signals about the quality and relevance of the web page.

The Physical Web feature is available on Chrome on iOS and Android. Users will need to turn on Bluetooth to use the feature.

If Android users have location settings enabled on both their device and in Chrome, they will receive a notification the first time they are near a beacon that will give them the option to turn on the Physical Web feature. This beacon's URL is not sent to Google's PWS unless the Physical Web feature is enabled. Users can also [enable](#) (or disable) the feature in the Privacy settings. Once a user enables the feature, Chrome scans for nearby devices for a few seconds each time the user unlocks the mobile device in use and sends them to the PWS in order to obtain more information about the beacon. The user receives a silent notification when Chrome finds a nearby URL.

On iOS devices, users can [enable](#) (or disable) the feature in the Privacy settings or by adding the [Chrome widget to their Today view](#) in the notification center. Additionally, the feature is automatically enabled for users who have location enabled on their device, granted Chrome the location permission, and have granted Google the geolocation permission. Chrome scans for nearby devices whenever it is open in the foreground. When Chrome finds nearby URLs, users will see them as omnibox suggestions. Additionally, Chrome scans for nearby devices for a few seconds when the Today widget is displayed in the notification center.

Google Chrome supports the [Web Bluetooth API](#), which provides websites with access to nearby [Bluetooth Low Energy devices](#) with your consent.

Chrome does not let any page communicate with a device unless you explicitly consent. When a web page asks to pair with a device, Chrome will ask you to choose which device the web page should access, if any. Selecting a device for one page does not give other pages access to the device you have chosen, and does not allow that page to access other devices. Currently, permission for a page to communicate with a device is usually revoked when the page is reloaded, and is always revoked when Chrome is restarted.

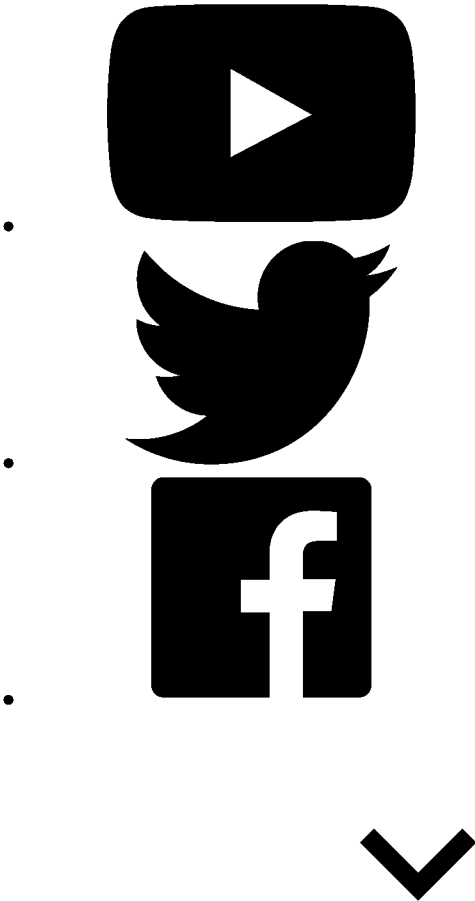
Chrome data that Android sends to Google

The data collection and usage described in this section is handled by Android and governed by the [Google Privacy Policy](#).

If the Android Backup Service is enabled on your device, some of your Chrome preferences will be saved and stored on Google servers. For Nexus and Android One devices, it is described under “Back up your data and settings with Android Backup Service” in [this article](#). For other Android devices, you may be able to find help by looking up your device on [this page](#). When setting up a new Android device, you may request that it copies the preferences from a previously set up device. If you do so, Android may restore backed up Chrome preferences when Chrome is first installed. The new device only copies the preferences if automatic restore is enabled (see “Restore your data and settings” in [the same article](#)), Chrome was signed into an account when the backup was made, and the new Android device is signed into that same account.

Chrome’s backup data for a particular device may also be restored if you uninstall and then later re-install Chrome on that device. This will only happen if automatic restore is enabled and the device is signed into the account that Chrome was signed into when the backup was made.

Follow us



Chrome Family

- [Other Platforms](#)
- [Chromebooks](#)
- [Chromecast](#)
- [Chrome Cleanup Tool](#)



Enterprise

- [Google Chrome Browser](#)
- [Devices](#)
- [Google Cloud](#)
- [G Suite](#)



Education

- [Google Chrome Browser](#)
- [Devices](#)
- [Web Store](#)



Dev and Partners

- [Chromium](#)
- [Chrome OS](#)
- [Chrome Web Store](#)
- [Chrome Experiments](#)
- [Chrome Beta](#)
- [Chrome Dev](#)
- [Chrome Canary](#)



Stay Connected

- [Google Chrome Blog](#)
- [Chrome Help](#)

Google

- [Privacy and Terms](#)
- [About Google](#)
- [Google Products](#)



[Help](#)

[Close](#)

Download Chrome for Windows

For Windows 10/8.1/8/7 32-bit.

For Windows 10/8.1/8/7 64-bit.

This computer will no longer receive Google Chrome updates because Windows XP and Windows Vista are no longer supported.

Download Chrome for Mac

For Mac OS X 10.10 or later.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

Download Chrome for Linux

Debian/Ubuntu/Fedora/openSUSE.

Please select your download package:

- ☒ 64 bit .deb (For Debian/Ubuntu)
- ☐ 64 bit .rpm (For Fedora/openSUSE)

Not Debian/Ubuntu or Fedora/openSUSE? There may be a community-supported version for your distribution [here](#).

Download Chrome for iOS

Google Chrome Terms of Service

These Terms of Service apply to the executable code version of Google Chrome. Source code for Google Chrome is available free of charge under open source software license agreements at <https://code.google.com/chromium/terms.html>.

1. Your relationship with Google

1.1 Your use of Google's products, software, services and web sites (referred to collectively as the "Services" in this document and excluding any services provided to you by Google under a separate written agreement) is subject to the terms of a legal agreement between you and Google. "Google" means Google Inc., whose principal place of business is at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States. This document explains how the agreement is made up, and sets out some of the terms of that agreement.

1.2 Unless otherwise agreed in writing with Google, your agreement with Google will always include, at a minimum, the terms and conditions set out in this document. These are referred to below as the "Universal Terms". Open source software licenses for Google Chrome source code constitute separate written agreements. To the limited extent that the open source software licenses expressly supersede these Universal Terms, the open source licenses govern your agreement with Google for the use of Google Chrome or specific included components of Google Chrome.

1.3 Your agreement with Google will also include the terms set forth below in the Google Chrome Additional Terms of Service and terms of any Legal Notices applicable to the Services, in addition to the Universal Terms. All of these are referred to below as the "Additional Terms". Where Additional Terms apply to a Service, these will be accessible for you to read either within, or through your use of, that Service.

1.4 The Universal Terms, together with the Additional Terms, form a legally binding agreement between you and Google in relation to your use of the Services. It is important that you take the time to read them carefully. Collectively, this legal agreement is referred to below as the "Terms".

1.5 If there is any contradiction between what the Additional Terms say and what the Universal Terms say, then the Additional Terms shall take precedence in relation to that Service.

2.1 In order to use the Services, you must first agree to the Terms. You may not use the Services if you do not accept the Terms.

2.2 You can accept the Terms by:

(A) clicking to accept or agree to the Terms, where this option is made available to you by Google in the user interface for any Service; or

(B) by actually using the Services. In this case, you understand and agree that Google will treat your use of the Services as acceptance of the Terms from that point onwards.

3. Language of the Terms

3.1 Where Google has provided you with a translation of the English language version of the Terms, then you agree that the translation is provided for your convenience only and that the English language versions of the Terms will govern your relationship with Google.

3.2 If there is any contradiction between what the English language version of the Terms says and what a translation says, then the English language version shall take precedence.

4. Provision of the Services by Google

4.1 Google has subsidiaries and affiliated legal entities around the world ("Subsidiaries and Affiliates"). Sometimes, these companies will be providing the Services to you on behalf of Google itself. You acknowledge and agree that Subsidiaries and Affiliates will be entitled to provide the Services to you.

4.2 Google is constantly innovating in order to provide the best possible experience for its users. You acknowledge and agree that the form and nature of the Services which Google provides may change from time to time without prior notice to you.

4.3 As part of this continuing innovation, you acknowledge and agree that Google may stop (permanently or temporarily) providing the Services (or any features within the Services) to you or to users generally at Google's sole discretion, without prior notice to you. You may stop using the Services at any time. You do not need to specifically inform Google when you stop using the Services.

4.4 You acknowledge and agree that if Google disables access to your account, you may be prevented from accessing the Services, your account details or any files or other content which is contained in your account.

5. Use of the Services by you

5.1 You agree to use the Services only for purposes that are permitted by (a) the Terms and (b) any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries).

5.2 You agree that you will not engage in any activity that interferes with or disrupts the Services (or the servers and networks which are connected to the Services).

5.3 Unless you have been specifically permitted to do so in a separate agreement with Google, you agree that you will not reproduce, duplicate, copy, sell, trade or resell the Services for any purpose.

5.4 You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) any breach of your obligations under the Terms and for the consequences (including any loss or damage which Google may suffer) of any such breach.

6. Privacy and your personal information

6.1 For information about Google's data protection practices, please read Google's privacy policy at <https://www.google.com/privacy.html> and at <https://www.google.com/intl/en/chrome/privacy/>. This policy explains how Google treats your personal information, and protects your privacy, when you use the Services.

6.2 You agree to the use of your data in accordance with Google's privacy policies.

7. Content in the Services

7.1 You understand that all information (such as data files, written text, computer software, music, audio files or other sounds, photographs, videos or other images) which you may have access to as part of, or through your use of, the Services are the sole responsibility of the person from which such content originated. All such information is referred to below as the "Content."

7.2 You should be aware that Content presented to you as part of the Services, including but not limited to advertisements in the Services and sponsored Content within the Services may be protected by intellectual property rights which are owned by the sponsors or advertisers who provide that Content to Google (or by other persons or companies on their behalf). You may not modify, rent, lease, loan, sell, distribute or create derivative works based on this Content (either in whole or in part) unless you have been specifically told that you may do so by Google or by the owners of that Content, in a separate agreement.

7.3 Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some of the Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings (see <https://support.google.com/websearch/answer/510?hl=en>). In addition, there are commercially available services and software to limit access to material that you may find objectionable.

7.4 You understand that by using the Services you may be exposed to Content that you may find offensive, indecent or objectionable and that, in this respect, you use the Services at your own risk.

7.5 You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) any Content that you create, transmit or display while using the Services and for the consequences of your actions (including any loss or damage which Google may suffer) by doing so.

8. Proprietary rights

8.1 You acknowledge and agree that Google (or Google's licensors) own all legal right, title and interest in and to the Services, including any intellectual property rights which subsist in the Services (whether those rights happen to be registered or not, and wherever in the world those rights may exist).

8.2 Unless you have agreed otherwise in writing with Google, nothing in the Terms gives you a right to use any of Google's trade names, trade marks, service marks, logos, domain names, and other distinctive brand features.

8.3 If you have been given an explicit right to use any of these brand features in a separate written agreement with Google, then you agree that your use of such features shall be in compliance with that agreement, any applicable provisions of the Terms, and Google's brand feature use guidelines as updated from time to time. These guidelines can be viewed online at <https://www.google.com/permissions/guidelines.html> (or such other URL as Google may provide for this purpose from time to time).

8.4 Google acknowledges and agrees that it obtains no right, title or interest from you (or your licensors) under these Terms in or to any Content that you submit, post, transmit or display on, or through, the Services, including any intellectual property rights which subsist in that Content (whether those rights happen to be registered or not, and wherever in the world those rights may exist). Unless you have agreed otherwise in writing with Google, you agree that you are responsible for protecting and enforcing those rights and that Google has no obligation to do so on your behalf.

8.5 You agree that you shall not remove, obscure, or alter any proprietary rights notices (including copyright and trade mark notices) which may be affixed to or contained within the Services.

8.6 Unless you have been expressly authorized to do so in writing by Google, you agree that in using the Services, you will not use any trade mark, service mark, trade name, logo of any company or organization in a way that is likely or intended to cause confusion about the owner or authorized user of such marks, names or logos.

9. License from Google

9.1 Google gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by Google as part of the Services as provided to you by Google (referred to as the "Software" below). This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Google, in the manner permitted by the Terms.

9.2 Subject to section 1.2, you may not (and you may not permit anyone else to) copy, modify, create a derivative work of, reverse engineer, decompile or otherwise attempt to extract the source code of the Software or any part thereof, unless this is expressly permitted or required by law, or unless you have been specifically told that you may do so by Google, in writing.

9.3 Subject to section 1.2, unless Google has given you specific written permission to do so, you may not assign (or grant a sub-license of) your rights to use the Software, grant a security interest in or over your rights to use the Software, or otherwise transfer any part of your rights to use the Software.

10. Content license from you

10.1 You retain copyright and any other rights you already hold in Content which you submit, post or display on or through, the Services.

11. Software updates

11.1 The Software which you use may automatically download and install updates from time to time from Google. These updates are designed to improve, enhance and further develop the Services and may take the form of bug fixes, enhanced functions, new software modules and completely new versions. You agree to receive such updates (and permit Google to deliver these to you) as part of your use of the Services.

12. Ending your relationship with Google

12.1 The Terms will continue to apply until terminated by either you or Google as set out below.

12.2 Google may at any time, terminate its legal agreement with you if:

(A) you have breached any provision of the Terms (or have acted in manner which clearly shows that you do not intend to, or are unable to comply with the provisions of the Terms); or

(B) Google is required to do so by law (for example, where the provision of the Services to you is, or becomes, unlawful); or

(C) the partner with whom Google offered the Services to you has terminated its relationship with Google or ceased to offer the Services to you; or

(D) Google is transitioning to no longer providing the Services to users in the country in which you are resident or from which you use the service; or

(E) the provision of the Services to you by Google is, in Google's opinion, no longer commercially viable.

12.3 Nothing in this Section shall affect Google's rights regarding provision of Services under Section 4 of the Terms.

12.4 When these Terms come to an end, all of the legal rights, obligations and liabilities that you and Google have benefited from, been subject to (or which have accrued over time whilst the Terms have been in force) or which are expressed to continue indefinitely, shall be unaffected by this cessation, and the provisions of paragraph 19.7 shall continue to apply to such rights, obligations and liabilities indefinitely.

13. EXCLUSION OF WARRANTIES

13.1 NOTHING IN THESE TERMS, INCLUDING SECTIONS 13 AND 14, SHALL EXCLUDE OR LIMIT GOOGLE'S WARRANTY OR LIABILITY FOR LOSSES WHICH MAY NOT BE LAWFULLY EXCLUDED OR LIMITED BY APPLICABLE LAW. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR CONDITIONS OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR LOSS OR DAMAGE CAUSED BY NEGLIGENCE, BREACH OF CONTRACT OR BREACH OF IMPLIED TERMS, OR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, ONLY THE LIMITATIONS WHICH ARE LAWFUL IN YOUR JURISDICTION WILL APPLY TO YOU AND OUR LIABILITY WILL BE LIMITED TO THE MAXIMUM EXTENT PERMITTED BY LAW.

13.2 YOU EXPRESSLY UNDERSTAND AND AGREE THAT YOUR USE OF THE SERVICES IS AT YOUR SOLE RISK AND THAT THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE."

13.3 IN PARTICULAR, GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO YOU THAT:

(A) YOUR USE OF THE SERVICES WILL MEET YOUR REQUIREMENTS,

(B) YOUR USE OF THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR,

(C) ANY INFORMATION OBTAINED BY YOU AS A RESULT OF YOUR USE OF THE SERVICES WILL BE ACCURATE OR RELIABLE, AND

(D) THAT DEFECTS IN THE OPERATION OR FUNCTIONALITY OF ANY SOFTWARE PROVIDED TO YOU AS PART OF THE SERVICES WILL BE CORRECTED.

13.4 ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICES IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR OTHER DEVICE OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL.

13.5 NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM GOOGLE OR THROUGH OR FROM THE SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TERMS.

13.6 GOOGLE FURTHER EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

14. LIMITATION OF LIABILITY

14.1 SUBJECT TO OVERALL PROVISION IN PARAGRAPH 13.1 ABOVE, YOU EXPRESSLY UNDERSTAND AND AGREE THAT GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS SHALL NOT BE LIABLE TO YOU FOR:

(A) ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL CONSEQUENTIAL OR EXEMPLARY DAMAGES WHICH MAY BE INCURRED BY YOU, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY.. THIS SHALL INCLUDE, BUT NOT BE LIMITED TO, ANY LOSS OF PROFIT (WHETHER INCURRED DIRECTLY OR INDIRECTLY), ANY LOSS OF GOODWILL OR BUSINESS REPUTATION, ANY LOSS OF DATA SUFFERED, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR OTHER INTANGIBLE LOSS;

(B) ANY LOSS OR DAMAGE WHICH MAY BE INCURRED BY YOU, INCLUDING BUT NOT LIMITED TO LOSS OR DAMAGE AS A RESULT OF:

(I) ANY RELIANCE PLACED BY YOU ON THE COMPLETENESS, ACCURACY OR EXISTENCE OF ANY ADVERTISING, OR AS A RESULT OF ANY RELATIONSHIP OR TRANSACTION BETWEEN YOU AND ANY ADVERTISER OR SPONSOR WHOSE ADVERTISING APPEARS ON THE SERVICES;

(II) ANY CHANGES WHICH GOOGLE MAY MAKE TO THE SERVICES, OR FOR ANY PERMANENT OR TEMPORARY CESSATION IN THE PROVISION OF THE SERVICES (OR ANY FEATURES WITHIN THE SERVICES);

(III) THE DELETION OF, CORRUPTION OF, OR FAILURE TO STORE, ANY CONTENT AND OTHER

(IV) YOUR FAILURE TO PROVIDE GOOGLE WITH ACCURATE ACCOUNT INFORMATION;

(V) YOUR FAILURE TO KEEP YOUR PASSWORD OR ACCOUNT DETAILS SECURE AND CONFIDENTIAL;

14.2 THE LIMITATIONS ON GOOGLE'S LIABILITY TO YOU IN PARAGRAPH 14.1 ABOVE SHALL APPLY WHETHER OR NOT GOOGLE HAS BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING.

15. Copyright and trade mark policies

15.1 It is Google's policy to respond to notices of alleged copyright infringement that comply with applicable international intellectual property law (including, in the United States, the Digital Millennium Copyright Act) and to terminating the accounts of repeat infringers. Details of Google's policy can be found at <https://www.google.com/dmca.html>.

15.2 Google operates a trade mark complaints procedure in respect of Google's advertising business, details of which can be found at https://www.google.com/tm_complaint.html.

16. Advertisements

16.1 Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.

16.2 The manner, mode and extent of advertising by Google on the Services are subject to change without specific notice to you.

16.3 In consideration for Google granting you access to and use of the Services, you agree that Google may place such advertising on the Services.

17. Other content

17.1 The Services may include hyperlinks to other web sites or content or resources. Google may have no control over any web sites or resources which are provided by companies or persons other than Google.

17.2 You acknowledge and agree that Google is not responsible for the availability of any such external sites or resources, and does not endorse any advertising, products or other materials on or available from such web sites or resources.

17.3 You acknowledge and agree that Google is not liable for any loss or damage which may be incurred by you as a result of the availability of those external sites or resources, or as a result of any reliance placed by you on the completeness, accuracy or existence of any advertising, products or other materials on, or available from, such web sites or resources.

18. Changes to the Terms

18.1 Google may make changes to the Universal Terms or Additional Terms from time to time. When these changes are made, Google will make a new copy of the Universal Terms available at https://www.google.com/intl/en/chrome/privacy/eula_text.html and any new Additional Terms will be made available to you from within, or through, the affected Services.

18.2 You understand and agree that if you use the Services after the date on which the Universal Terms or Additional Terms have changed, Google will treat your use as acceptance of the updated Universal Terms or Additional Terms.

19. General legal terms

19.1 Sometimes when you use the Services, you may (as a result of, or in connection with your use of the Services) use a service or download a piece of software, or purchase goods, which are provided by another person or company. Your use of these other services, software or goods may be subject to separate terms between you and the company or person concerned. If so, the Terms do not affect your legal relationship with these other companies or individuals.

19.2 The Terms constitute the whole legal agreement between you and Google and govern your use of the Services (but excluding any services which Google may provide to you under a separate written agreement), and completely replace any prior agreements between you and Google in relation to the Services.

19.3 You agree that Google may provide you with notices, including those regarding changes to the Terms, by email, regular mail, or postings on the Services.

19.4 You agree that if Google does not exercise or enforce any legal right or remedy which is contained in the Terms (or which Google has the benefit of under any applicable law), this will not be taken to be a formal waiver of Google's rights and that those rights or remedies will still be available to Google.

19.5 If any court of law, having the jurisdiction to decide on this matter, rules that any provision of these Terms is invalid, then that provision will be removed from the Terms without affecting the rest of the Terms. The remaining provisions of the Terms will continue to be valid and enforceable.

19.6 You acknowledge and agree that each member of the group of companies of which Google is the parent shall be third party beneficiaries to the Terms and that such other companies shall be entitled to directly enforce, and rely upon, any provision of the Terms which confers a benefit on (or rights in favor of) them. Other than this, no other person or company shall be third party beneficiaries to the Terms.

19.7 The Terms, and your relationship with Google under the Terms, shall be governed by the laws of the State of California without regard to its conflict of laws provisions. You and Google agree to submit to the exclusive jurisdiction of the courts located within the county of Santa Clara, California to resolve any legal matter arising from the Terms. Notwithstanding this, you agree that Google shall still be allowed to apply for injunctive remedies (or an equivalent type of urgent legal relief) in any jurisdiction.

20. Additional Terms for Extensions for Google Chrome

20.1 These terms in this section apply if you install extensions on your copy of Google Chrome. Extensions are small software programs, developed by Google or third parties, that can modify and enhance the functionality of Google Chrome. Extensions may have greater privileges to access your browser or your computer than regular webpages, including the ability to read and modify your private data.

20.2 From time to time, Google Chrome may check with remote servers (hosted by Google or by third parties) for available updates to extensions, including but not limited to bug fixes or enhanced functionality. You agree that such updates will be automatically requested, downloaded, and installed without further notice to you.

20.3 From time to time, Google may discover an extension that violates Google developer terms or other legal agreements, laws, regulations or policies. Google Chrome will periodically download a list of such extensions from Google's servers. You agree that Google may remotely disable or remove any such extension from user systems in its sole discretion.

21. Additional Terms for Enterprise Use

21.1 If you are a business entity, then the individual accepting on behalf of the entity (for the avoidance of doubt, for business entities, in these Terms, "you" means the entity) represents and warrants that he or she has the authority to act on your behalf, that you represent that you are duly authorized to do business in the country or countries where you operate, and that your employees, officers, representatives, and other agents accessing the Service are duly authorized to access Google Chrome and to legally bind you to these Terms.

21.2 Subject to the Terms, and in addition to the license grant in Section 9, Google grants you a non-exclusive, non-transferable license to reproduce, distribute, install, and use Google Chrome solely on machines intended for use by your employees, officers, representatives, and agents in connection with your business entity, and provided that their use of Google Chrome will be subject to the Terms.

August 12, 2010

Google Chrome Additional Terms of Service

MPEG LA

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PARTNER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Adobe

Google Chrome may include one or more components provided by Adobe Systems Incorporated and Adobe Software Ireland Limited (collectively "Adobe"). Your use of the Adobe software as provided by Google ("Adobe Software") is subject to the following additional terms (the "Adobe Terms"). You, the entity receiving the Adobe Software, will be hereinafter referred to as "Sublicensee."

1. License Restrictions.

(a) Flash Player, Version 10.x is designed only as a browser plug-in. Sublicensee may not modify or distribute this Adobe Software for use as anything but a browser plug-in for playing back content on a web page. For example, Sublicensee will not modify this Adobe Software in order to allow interoperation with applications that run outside of the browser (e.g., standalone applications, widgets, device UI).

(b) Sublicensee will not expose any APIs of the Flash Player, Version 10.x through a browser plug-in interface in such a way that allows such extension to be used to playback content from a web page as a stand-alone application.

(c) The Chrome-Reader Software may not be used to render any PDF or EPUB documents that utilize digital rights management protocols or systems other than Adobe DRM.

(d) Adobe DRM must be enabled in the Chrome-Reader Software for all Adobe DRM protected PDF and EPUB documents.

(e) The Chrome Reader Software may not, other than as explicitly permitted by the technical specifications, disable any capabilities provided by Adobe in the Adobe Software, including but not limited to, support for PDF and EPUB formats and Adobe DRM.

2. Electronic Transmission. Sublicensee may allow the download of the Adobe Software from a web site, the Internet, an intranet, or similar technology (an, "Electronic Transmissions") provided that Sublicensee agrees that any distributions of the Adobe Software by Sublicensee, including those on CD-ROM, DVD-ROM or other storage media and Electronic Transmissions, if expressly permitted, shall be subject to reasonable security measures to prevent unauthorized use. With relation to Electronic Transmissions approved hereunder, Sublicensee agrees to employ any reasonable use restrictions set by Adobe, including those related to security and/or the restriction of distribution to end users of the Sublicensee Product.

3. EULA and Distribution Terms.

(a) Sublicensee shall ensure that the Adobe Software is distributed to end users under an enforceable end user license agreement, in favor of Sublicensee and its suppliers containing at least each of the following minimum terms (the "End-User License"): (i) a prohibition against distribution and copying, (ii) a prohibition against modifications and derivative works, (iii) a prohibition against decompiling, reverse engineering, disassembling, and otherwise reducing the Adobe Software to a human-perceivable form, (iv) a provision indicating ownership of Sublicensee Product (as defined in Section 8) by Sublicensee and its licensors, (v) a disclaimer of indirect, special, incidental, punitive, and consequential damages, and (vi) other industry standard disclaimers and limitations, including, as applicable: a disclaimer of all applicable statutory warranties, to the full extent allowed by law.

(b) Sublicensee shall ensure that the Adobe Software is distributed to Sublicensee's distributors under an enforceable distribution license agreement, in favor of Sublicensee and its suppliers containing terms as protective of Adobe as the Adobe Terms.

4. Opensource. Sublicensee will not directly or indirectly grant, or purport to grant, to any third party any rights or immunities under Adobe's intellectual property or proprietary rights that will subject such intellectual property to an open source license or scheme in which there is or could be interpreted to be a requirement that as a condition of use, modification and/or distribution, the Adobe Software be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; or (iii) redistributable at no charge. For clarification purposes, the foregoing restriction does not preclude Sublicensee from distributing, and Sublicensee will distribute the Adobe Software as bundled with the Google Software, without charge.

5. Additional Terms. With respect to any update, upgrade, new versions of the Adobe Software (collectively "Upgrades") provided to Sublicensees, Adobe reserves the right to require additional terms and conditions applicable solely to the Upgrade and future versions thereof, and solely to the extent that such restrictions are imposed by Adobe on all licensees of such Upgrade. If Sublicensee does not agree to such additional terms or conditions, Sublicensee will have no license rights with respect to such Upgrade, and Sublicensee's license rights with respect to the Adobe Software will terminate automatically on the 90th day from the date such additional terms are made available to Sublicensee.

6. Proprietary Rights Notices. Sublicensee shall not, and shall require its distributors not to, delete or in any manner alter the copyright notices, trademarks, logos or related notices, or other proprietary rights notices of Adobe (and its licensors, if any) appearing on or within the Adobe Software or accompanying materials.

7. Technical Requirements. Sublicensee and its distributors may only distribute Adobe Software and/or Upgrade on devices that (i) meet the technical specifications posted on <http://www.adobe.com/mobile/licensees>, (or a successor web site thereto), and (ii) has been verified by Adobe as set forth below.

8. Verification and Update. Sublicensee must submit to Adobe each Sublicensee product (and each version thereof) containing the Adobe Software and/or Upgrade ("Sublicensee Product") that do not meet the Device Verification exemption criteria to be communicated by Google, for Adobe to verify. Sublicensee shall pay for each submission made by Sublicensee by procuring verification packages at Adobe's then-current terms set forth at <http://flashmobile.adobe.com/>. Sublicensee Product that has not passed verification may not be distributed. Verification will be accomplished in accordance with Adobe's then-current process described at <http://flashmobile.adobe.com/> ("Verification").

9. Profiles and Device Central. Sublicensee will be prompted to enter certain profile information about the Sublicensee Products either as part of the Verification process or some other method, and Sublicensee will provide such information, to Adobe. Adobe may (i) use such profile information as reasonably necessary to verify the Sublicensee Product (if such product is subject to Verification), and (ii) display such profile information in "Adobe Device Intelligence system," located at <https://devices.adobe.com/partnerportal/>, and made available through Adobe's authoring and development tools and services to enable developers and end users to see how content or applications are displayed in Sublicensee Products (e.g. how video images appear in certain phones).

10. Export. Sublicensee acknowledges that the laws and regulations of the United States restrict the export and re-export of commodities and technical data of United States origin, which may include the Adobe Software. Sublicensee agrees that it will not export or re-export the Adobe Software, without the appropriate United States and foreign governmental clearances, if any.

11. Technology Pass-through Terms.

(a) Except pursuant to applicable permissions or agreements therefor, from or with the applicable parties, Sublicensees shall not use and shall not allow the use of, the Adobe Software for the encoding or decoding of mp3 audio only (.mp3) data on any non-pc device (e.g., mobile phone or set-top box), nor may the mp3 encoders or decoders contained in the Adobe Software be used or accessed by any product other than the Adobe Software. The Adobe Software may be used

for the encoding or decoding of MP3 data contained within a swf or flv file, which contains video, picture or other data. Sublicensee shall acknowledge that use of the Adobe Software for non-PC devices, as described in the prohibitions in this section, may require the payment of licensing royalties or other amounts to third parties who may hold intellectual property rights related to the MP3 technology and that Adobe nor Sublicensee has not paid any royalties or other amounts on account of third party intellectual property rights for such use. If Sublicensee requires an MP3 encoder or decoder for such use, Sublicensee is responsible for obtaining the necessary intellectual property license, including any applicable patent rights.

(b) Sublicensee will not use, copy, reproduce and modify (i) the On2 source code (provided hereunder as a component of the Source Code) as necessary to enable the Adobe Software to decode video in the Flash video file format (.flv or .f4v), and (ii) the Sorenson Spark source code (provided hereunder as a component of the Source Code) for the limited purpose of making bug fixes and performance enhancements to the Adobe Software. All codecs provided with the Adobe Software may only be used and distributed as an integrated part of the Adobe Software and may not be accessed by any other application, including other Google applications.

(c) The Source Code may be provided with an AAC codec and/or HE-AAC codec ("the AAC Codec"). Use of the AAC Codec is conditioned on Sublicensee obtaining a proper patent license covering necessary patents as provided by VIA Licensing, for end products on or in which the AAC Codec will be used. Sublicensee acknowledges and agrees that Adobe is not providing a patent license for an AAC Codec under this Agreement to Sublicensee or its sublicensees.

(d) THE SOURCE CODE MAY CONTAIN CODE LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR WILL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. See <http://www.mpegla.com>

12. Update. Sublicensee will not circumvent Google's or Adobe's efforts to update the Adobe Software in all Sublicensee's products incorporating the Adobe Software as bundled with the Google Software ("Sublicensee Products").

13. Attribution and Proprietary Notices. Sublicensee will list the Adobe Software in publicly available Sublicensee Product specifications and include appropriate Adobe Software branding (specifically excluding the Adobe corporate logo) on the Sublicensee Product packaging or marketing materials in a manner consistent with branding of other third party products contained within the Sublicensee Product.

14. No Warranty. THE ADOBE SOFTWARE IS MADE AVAILABLE TO SUBLICENSEE FOR USE AND REPRODUCTION "AS IS" AND ADOBE MAKES NO WARRANTY AS TO ITS USE OR PERFORMANCE. ADOBE AND ITS SUPPLIERS DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS OBTAINED BY USING THE ADOBE SOFTWARE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO SUBLICENSEE IN SUBLICENSEE'S JURISDICTION, ADOBE AND ITS SUPPLIERS MAKE NO WARRANTIES, CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING WITHOUT LIMITATION NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, SATISFACTORY QUALITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. SUBLICENSEE AGREES THAT SUBLICENSEE SHALL NOT MAKE ANY WARRANTY, EXPRESS OR IMPLIED, ON BEHALF OF ADOBE.

15. Limitation of Liability. IN NO EVENT WILL ADOBE OR ITS SUPPLIERS BE LIABLE TO SUBLICENSEE FOR ANY DAMAGES, CLAIMS OR COSTS WHATSOEVER OR ANY CONSEQUENTIAL, INDIRECT, OR INCIDENTAL DAMAGES, OR ANY LOST PROFITS OR LOST SAVINGS, EVEN IF AN ADOBE REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS, DAMAGES, CLAIMS OR COSTS OR FOR ANY CLAIM BY ANY THIRD PARTY. THE FOREGOING LIMITATIONS AND EXCLUSIONS APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW IN SUBLICENSEE'S JURISDICTION. ADOBE'S AGGREGATE LIABILITY AND THAT OF ITS SUPPLIERS UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO ONE THOUSAND DOLLARS (US\$1,000). Nothing contained in this Agreement limits Adobe's liability to Sublicensee in the event of death or personal injury resulting from Adobe's negligence or for the tort of deceit (fraud). Adobe is acting on behalf of its suppliers for the purpose of disclaiming, excluding and/or limiting obligations, warranties and liability as provided in this Agreement, but in no other respects and for no other purpose.

16. Content Protection Terms

(a) Definitions.

"Compliance and Robustness Rules" means the document setting forth compliance and robustness rules for the Adobe Software located at <http://www.adobe.com/mobile/licensees>, or a successor web site thereto.

"Content Protection Functions" means those aspects of the Adobe Software that are designed to ensure compliance with the Compliance and Robustness Rules, and to prevent playback, copying, modification, redistribution or other actions with respect to digital content distributed for consumption by users of the Adobe Software when such actions are not authorized by the owners of such digital content or its licensed distributors.

"Content Protection Code" means code within certain designated versions of the Adobe Software that enables certain Content Protection Functions.

"Key" means a cryptographic value contained in the Adobe Software for use in decrypting digital content.

(b) License Restrictions. Sublicensee's right to exercise the licenses with respect to the Adobe Software is subject to the following additional restrictions and obligations. Sublicensee will ensure that Sublicensee's customers comply with these restrictions and obligations to the same extent imposed on Sublicensee with respect to the Adobe Software; any failure by Sublicensee's customers to comply with these additional restrictions and obligations shall be treated as a material breach by Sublicensee.

b.1. Sublicensee and customers may only distribute the Adobe Software that meets the Robustness and Compliance Rules as so confirmed by Sublicensee during the verification process described above in the Adobe Terms.

b.2. Sublicensee shall not (i) circumvent the Content Protection Functions of either the Adobe Software or any related Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software or (ii) develop or distribute products that are designed to circumvent the Content Protection Functions of either the Adobe Software or any Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software.

(c) The Keys are hereby designated as Adobe's Confidential Information, and Sublicensee will, with respect to the Keys, adhere to Adobe's Source Code Handling Procedure (to be provided by Adobe upon request).

(d) Injunctive Relief. Sublicensee agrees that a breach of this Agreement may compromise the Content Protection Functions of the Adobe Software and may cause unique and lasting harm to the interests of Adobe and owners of digital content that rely on such Content Protection Functions, and that monetary damages may be inadequate to compensate fully for such harm. Therefore, Sublicensee further agrees that Adobe may be entitled to seek injunctive relief to prevent or limit the harm caused by any such breach, in addition to monetary damages.

17. Intended Third-party Beneficiary. Adobe Systems Incorporated and Adobe Software Ireland Limited are the intended third-party beneficiaries of Google's agreement with Sublicensee with respect to the Adobe Software, including but not limited to, the Adobe Terms. Sublicensee agrees, notwithstanding anything to the contrary in its agreement with Google, that Google may disclose Sublicensee's identity to Adobe and certify in writing that Sublicensee has entered into a license agreement with Google which includes the Adobe Terms. Sublicensee must have an agreement with each of its licensees, and if such licensees are allowed to redistribute the Adobe Software, such agreement will include the Adobe Terms.

[Printer-friendly version](#)

Note: Installing Google Chrome will **add the Google repository** so your system will automatically keep Google Chrome up to date. If you don't want Google's repository, do "sudo touch /etc/default/google-chrome" before installing the package.

☒ Set Google Chrome as my default browser

☒ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. [Learn more](#)

Accept and Install 

Download Chrome

Download for Windows

For Windows 10/8.1/8/7 32-bit

For Windows 10/8.1/8/7 64-bit

This computer will no longer receive Google Chrome updates because Windows XP and Windows Vista are no longer supported.

Download for Mac

Mac OS X 10.10 or later

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

Download for Linux

Debian/Ubuntu/Fedora/openSUSE

Download for phone or tablet

- [Android](#)
- [iOS](#)

Download for another desktop OS

- [Windows 10/8.1/8/7 64-bit](#)

- Windows 10/8.1/8/7-32-bit
- Mac OS X 10.10 or later
- Linux

Frozen versions

- Windows XP
- Windows Vista
- Mac 10.6 - 10.8
- Mac 10.9

Looks like you're already using Chrome browser. Nice!

The device you have runs on Chrome OS, which already has Chrome browser built-in. No need to manually install or update it — with automatic updates, you'll always get the latest version. [Learn more about automatic updates.](#)

Looking for Chrome for a different operating system?

See the [full list of supported operating systems.](#)

EXHIBIT 22



Go g e

[Chrome](#)

[Skip to content](#)

- [Features](#)
 - [Productivity](#)
 - [Google built-in](#)
 - [Security](#)
 - [Anywhere](#)
- [Do More with Chrome](#)
- [Extensions](#)
- [Enterprise](#)

Download Chrome

Go g e

[Chrome](#)

- [Features](#)
 - [Productivity](#)
 - [Google built-in](#)
 - [Security](#)
 - [Anywhere](#)
- [Do More with Chrome](#)
- [Extensions](#)
- [Enterprise](#)

Google Chrome Privacy Whitepaper

Last modified: January 29, 2019 (Current as of Chrome 72.0.3626.96)

- [Omnibox](#)
- [Network predictions](#)
- [Search locale](#)
- [New Tab page](#)
- [Tap to Search](#)
- [More like this](#)
- [Safe Browsing protection](#)
- [Unwanted software protection](#)
- [Navigation errors](#)
- [Offline Indicator](#)
- [Google update](#)
- [Network time](#)
- [Counting install](#)
- [Measuring promotions](#)
- [Usage stats](#)
- [Google Surveys](#)
- [Spelling suggestions](#)
- [Translate](#)
- [Signing In](#)
- [Autofill](#)
- [Payments](#)

- [Geolocation](#)
- [Speech to text](#)
- [Google Assistant](#)
- [Cloud Print](#)
- [SSL certificate error reporting](#)
- [Installed apps](#)
- [Push Messaging](#)
- [Chrome custom tabs](#)
- [Continue where you left off](#)
- [Chrome variations](#)
- [Do Not Track](#)
- [Plugins](#)
- [Media licenses](#)
- [Cloud policy](#)
- [Data Saver \(Chrome mobile\)](#)
- [Supervised users](#)
- [Kid's Google Account](#)
- [Incognito and Guest mode](#)
- [Handoff support](#)
- [Security key](#)
- [Physical web](#)
- [Bluetooth](#)
- [Data sent by Android](#)

This document describes the features in Chrome that communicate with Google, as well as with third-party services (for example, if you've changed your default search engine). This document also describes the controls available to you regarding how your data is used by Chrome. Here we're focusing on the desktop version of Chrome; we touch only tangentially on Chrome OS and Chrome for Mobile. This document does not cover features that are still under development, such as features in the beta, dev and canary channel and active field trials, or Android apps on Chrome OS if Play Apps are enabled.

If you have questions about Google Chrome and Privacy that this document doesn't answer, please contact the privacy team at privacy@chromium.org. We'd be happy to hear from you.

Omnibox

Google Chrome uses a combined [web address and search bar](#) (we call it the "omnibox") at the top of the browser window.

As you use the omnibox, your [default search engine](#) can suggest addresses and search queries that may be of interest to you. These suggestions make navigation and searching faster and easier, and are turned on by default. They can be turned off by unchecking "Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box" in the "Privacy" section of Chrome's settings. They are also disabled in incognito mode.



In order to provide these suggestions, Chrome sends the text you've typed into the omnibox, along with a general categorization (e.g., "URL", "search query", or "unknown"), to your default search engine. Chrome will also send a signal to your default search provider when you focus in the omnibox, telling it to get ready to provide suggestions. Your IP address and certain cookies are also sent to your default search engine with all requests, in order to return the results that are most relevant to you.

If Chrome determines that your typing may contain sensitive information, such as authentication credentials, local file names, or URL data that is normally encrypted, it will not send the typed text.

If Google is your default search engine, when you select one of the omnibox suggestions, Chrome sends your original search query, the suggestion you selected, and the position of the suggestion back to Google. This information helps improve the quality of the suggestion feature, and it's logged and anonymized in the same manner as Google web searches. Logs of these suggestion requests are retained for two weeks, after which 2% of the log data is randomly selected, anonymized, and retained in order to improve the suggestion feature.

If you've chosen to sync your Chrome history, and if Google is your default search engine, the URL of the page you're viewing is sent to Google in order to provide better, contextually relevant suggestions. URLs are sent only for HTTP pages and HTTPS pages, not other schemes such as file: and ftp:. Additionally, Chrome may present suggestions as soon as you place the cursor in the omnibox, before you start typing. Chrome is in the process of transitioning to a new service to provide these on-focus suggestions. For most users on desktop versions of Chrome, the request and complete set of suggestions are retained on Google servers in order to further improve and personalize the feature. When the URL that triggered the set of suggestions is deleted from your history, the set of suggestions will stop influencing suggestions personalized to you, and will be deleted; otherwise they are retained in your Google account for a year. For a small portion of users on desktop versions of Chrome, and users on mobile versions of Chrome, the logging described in the previous paragraphs apply except that URLs are never included in the 2% sampling of log data.

On Android, your location will also be sent to Google via an X-Geo HTTP request header if Google is your default search engine, the Chrome app has the permission to use your geolocation and you haven't blocked geolocation for www.google.com (or country-specific origins such as www.google.de). Additionally, if your device has network location

enabled (High Accuracy or Battery Saving Device Location mode in Android settings), the X-Geo header may also include visible network IDs (WiFi and Cell), used to geocode the request server-side. The X-Geo header will never be sent in Incognito mode. HTTPS will be required to include this header in the request. You can learn more about how to control the Android OS location sharing with apps on [this article](#) for Nexus, or find your device [here](#) if you do not use a Nexus. How to control location sharing with a site within Chrome is written in [this article](#). See the [Geolocation](#) section of this whitepaper for more information on default geolocation permissions.

Additionally, if Google is your search engine and you have enabled sync, omnibox may also show suggestions for your Google Drive files. You can turn this functionality off by disabling the “Drive suggestions” option in Sync settings.

If you use a non-Google search provider as your default search engine, queries are sent and logged under that provider's privacy policy.

Additionally, when you use the omnibox to search for a single word, Chrome may send this word to your DNS server to see whether it corresponds to a host on your network, and may try to connect to the corresponding host. This gives you the option to navigate to that host instead of searching. For example, if your router goes by the hostname “router”, and you type “router” in the omnibox, you’re given the option to navigate to <https://router/>, as well as to search for the word “router” with your default search provider. This feature is not controlled by the “Use a prediction service to help complete searches and URLs...” option because it does not involve sending data to your default search engine.

Network predictions

Chrome uses a prediction service to load pages more quickly. The prediction service uses navigation history and local heuristics to predict which resources and pages are likely to be needed next, and it initiates actions such as DNS prefetching, TCP and TLS preconnection, and prefetching of web pages. To [turn off](#) network predictions, uncheck “Use a prediction service to load pages more quickly” in the “Privacy” section of Chrome’s settings.

To improve load times, the browser can be asked to prefetch links that you might click next. Chrome supports four types of prefetching:

- Chrome prefetching - can be initiated by Chrome itself whenever it detects a search query typed in the omnibox or a likely beginning of a URL you type often
- Webpage prefetching - requested by one web page to prefetch another
- AMP prefetching - can be requested only by the Google Search App on Android to prefetch several accelerated mobile pages (AMP) articles and display them later in a Chrome Custom Tab
- CustomTabs prefetching - any Android app can request to prefetch several URLs to speed up displaying them later in a Chrome Custom Tab

Controlling the feature. All prefetching types except webpage prefetching are controlled by Chrome’s prediction service setting. Webpage prefetching is allowed regardless of whether Chrome’s network prediction service feature is enabled.

Handling of cookies. The prefetched site is allowed to set and read its own cookies just as if you had visited it (even if you don’t end up visiting the prefetched page). All types of prefetching are disabled if you disallow third party cookies to prevent cookies from being set from pages that you did not visit.

Javascript execution. For AMP prefetching the page is fully rendered and Javascript is also executed. For the remaining types of prefetching Javascript is not executed.

Google search locale

If Google is set as your default search engine, Chrome will try to determine the most appropriate locale for Google search queries conducted from the [omnibox](#) in order to give you relevant search results based on your location. For example, if you were in Germany, your omnibox searches may go through google.de instead of google.com.

In order to do this, Chrome will send a request to google.com each time you start the browser. If you already have any cookies from the google.com domain, this request will also include these cookies, and is logged as any normal HTTPS request to google.com would be (see the [description of “server logs” in the privacy key terms](#) for details). If you do not have any cookies from google.com, this request will not create any.

New Tab page

The Chrome New Tab page may display suggestions for websites that you might want to visit.

In order to help you get started, Chrome may suggest content that is popular in your country or region. Chrome uses your IP address to identify your country or region.

Chrome tries to make personalized suggestions that are useful to you. For this, Chrome uses the sites you have visited from your local browsing history. On Android, the most popular languages of the sites you visited may also be sent to Google to provide suggestions in languages you prefer to read, and the device display DPI may be sent to format content for your device. To save data, Chrome may additionally send a hash of the content that Google provided to you the last time, so that you only download content when there is something new.

If you are signed into Chrome, suggestions are *also* based on data stored in your Google account activity. You can control the collection of data in your Google account at [Activity controls](#) and manage your account activity at [My Activity](#). For example, if you sync your browsing history and have enabled its use in your Web & App activity, Google

may suggest sites that relate to sites you have visited in the past. Chrome measures the quality of suggestions by sending Google information about the sets of suggestions that were displayed, and those that were selected.

On the desktop version of Chrome, you may also manually add shortcuts to websites that you regularly visit, or edit Chrome's existing website suggestions. After you add, edit, or delete a shortcut to a website, the Chrome New Tab page will not suggest any new websites to you.

Suggestions generated from your browsing history will be removed once you clear your browsing history. However, if you customized your suggestions, they will not be removed.

For Chrome on Android, in certain countries, Chrome may download the content of the New Tab page suggestions from Google, for use while offline. Chrome sends to Google a cookieless request with the URL for each suggestion, along with Chrome's user agent string, in order to render the content. You can remove downloaded content by clearing Chrome's cache data, or by opening the Downloads menu and selecting individual pages to delete. You can disable this feature by disabling "Automatically download pages" in Chrome's Privacy settings.

For desktop and Android versions of Chrome, when you open a new tab, Chrome loads a New Tab page customized by your default search engine (e.g., google.com) if it's available. This page is preloaded in the background and refreshed periodically so that it opens quickly. Your IP address and cookies, as well as your current browser theme, are sent to your search engine with each refresh request so that the New Tab page can be correctly displayed. See the Embedded Search API for more details. Your search engine may also record your interactions with the New Tab page.

The New Tab page content may be designed by your default search provider. Suggested websites are embedded by Chrome into the New Tab page in a way that does not expose them to your default search provider.

This information about the New Tab page may not apply if you've installed an extension that overrides the New Tab page.

Tap to Search

If you've enabled "Tap to Search" on Chrome Mobile you can search for terms by tapping them.

When you tap a word, the word, the surrounding text, and the home country of your device's SIM card are sent to Google to identify recommended search terms (for example, tapping on "Michael" on a site about Michael Jackson might lead to a suggested search for "Michael Jackson"). The tapped word is logged in accordance with standard Google logging policies, and the surrounding text and home country are logged only when the page is already in Google's search index. If you sync your browsing history, the URL of the page is also sent and logged, and is used to improve your query suggestions.

When Google returns a search suggestion, a card "peeks through" at the bottom of the screen, showing the suggested search term. Opening this card is considered a regular search and navigation on Google, so standard logging policies apply.

Long-pressing on a word opens a peeking card with the selected word, except on recent versions of Android Oreo and higher which activates Smart Text Selection instead. No communication with Google occurs until the card is opened, and no surrounding text is sent. Saying "Ok Google" after long-pressing on a word provides the word and its surrounding text as context for the Google Assistant.

Tap to Search is enabled in a limited mode by default: potentially privacy-sensitive data, such as the URL and surrounding text, is not sent for HTTPS pages. Tap to Search can be fully enabled and disabled in the card or in the Chrome privacy settings.

More like this

If you have chosen to sync your browsing history, Chrome may provide contextually relevant content recommendations on certain pages via a "More like this" button on the top toolbar and the suggestions will be shown from a bottom sheet.

In order to provide these suggestions, the URL of the page that you're currently viewing, along with your language or locale information and IP address is sent to Google. Suggestions are only fetched for HTTP and HTTPS pages, not pages with other schemas like file: or ftp:. Selected suggestions are logged in accordance with standard Google logging policies.

Suggestions are not available on all webpages. When there are suggestions, the "More like this" button will appear on the top toolbar.

Safe Browsing protection

Google Chrome includes an optional feature called "Safe Browsing" to help protect you against phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. You can find more information at safebrowsing.google.com about how Safe Browsing protects you in Chrome and other Google products. Safe Browsing is designed specifically to protect your privacy and is also used by other popular browsers. This feature is not available on the iOS version of Chrome.

When Safe Browsing is enabled in Chrome, Chrome contacts Google's servers periodically to download the most recent Safe Browsing list of unsafe extensions and sites, including phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. The most recent copy of this list is stored locally on

your system. Chrome checks the URL of each site you visit or file you download against this local list. If you navigate to a URL that appears on the list, Chrome sends a partial URL fingerprint (the first 32 bits of a SHA-256 hash of the URL) to Google for verification that the URL is indeed dangerous. Chrome also sends a partial URL fingerprint when a site requests a potentially dangerous permission, so that Google can protect you if the site is malicious. Google cannot determine the actual URL from this information.

In addition to the URL check described above, Chrome also conducts client-side checks. If a website looks suspicious, Chrome sends a subset of likely phishing and social engineering terms found on the page to Google, in order to determine whether the website should be considered malicious. Chrome can also help protect you from phishing if you type one of your previously saved passwords into an uncommon site. In this case Chrome sends the URL and referrers of the page to Google to see if the page might be trying to steal your password.

If you encounter a website that is on Chrome's Safe Browsing list, you may see a warning like the one shown below. From there, you can choose to opt in to reporting data relevant to security to help improve Safe Browsing and security on the Internet. If you opt in, an incident report will be sent every time you receive a warning or visit a suspicious page. Chrome is currently transitioning this opt-in to change the reporting functionality. If your checkbox reads "Automatically send some system information and page content to Google to help detect dangerous apps and sites" then you are part of the new group of users. This setting differs from the old "report security incidents to Google" in that security reports will also be sent on a very small sample of other sites to help Safe Browsing learn about new threats you may be encountering. This new setting will be unchecked by default even if you opted in to the older setting. The reports are sent to Google over an encrypted channel and can include URLs, headers, and snippets of content from the page and they never include data from browsing you do in Incognito mode. In cases where Chrome discovers unwanted or malicious software on your machine, the reports may also include details about malicious files and registry entries. This data is used only to improve Safe Browsing and to improve security on the Internet. For example, Chrome reports some SSL certificate chains to Google to help improve the accuracy of Chrome's SSL warnings.



You can visit our malware warning test page or social engineering warning test page to see the above example in action. For more information about the warning pages, see Manage warnings about unsafe sites. You can find settings for Safe Browsing and the additional reports in the Privacy section of Chrome settings. Please be aware that if you disable the Safe Browsing feature, Chrome will no longer be able to protect you from websites that try to steal your information or install harmful software. We don't recommend turning it off.

If you are a webmaster, developer, or network admin, you can find more relevant information about Safe Browsing on this page.

Safe Browsing also protects you from abusive extensions and malicious software. At start up of Chrome, Safe Browsing scans extensions installed in your browser against the Safe Browsing list. If an extension on the list is found, Chrome will temporarily disable the extension, offer you relevant information and provide an option for you to remove the extension or re-enable it. Chrome also sends the particular extension ID to Safe Browsing. If you attempt to download a file on Chrome's Safe Browsing list, you'll see a warning like this one:



To warn you about potentially dangerous files, like the picture shown above, Chrome checks the URL of potentially dangerous file types you download against a list of URLs that have been verified. This list is stored locally on your computer and updated regularly. Chrome does not send information to Google for files you download from URLs in this list, or if the file is signed by a verified publisher. For all other unverified potentially dangerous file downloads, Chrome sends Google the information needed to help determine whether the download is harmful, including some or all of the following: information about the full URL of the site or file download, all related referrers and redirects, code signing certificates, file hashes, and file header information. Chrome may then show a warning like the one pictured above.

Chrome helps protect you against password phishing by checking with Google when you enter your password on an uncommon page. Chrome keeps a local list of popular websites that Safe Browsing found to be safe. If Chrome detects that you have entered your Google account password or one of your passwords stored in Chrome's password manager on a website that's not on the list, it sends a request to Safe Browsing to gather the reputation of that website. The verdict received from Safe Browsing is usually cached on your device for 1 week.

If the reused password is your Google account password and the verdict for the website is that it is phishing, Chrome will suggest that you change your Google account password to avoid losing access to your account. Additionally, if you sync your browsing history without a sync passphrase, Chrome sends another request to tell Google that your password was likely phished, to make hijacking of your Google account by an adversary more difficult. The information sent in this request includes the ID of the synced browsing history entry to identify the URL where the phishing attempt happened, and the verdict received from Safe Browsing.

If you've opted into sharing data relevant to security to help detect dangerous apps and sites, Chrome also sends a request to Safe Browsing each time you start to enter a password on a page that isn't in Chrome's local list. In addition, the request that Chrome sends to Safe Browsing to determine the reputation of the website on which you reuse your password includes the list of websites for which you saved this password in Chrome's password manager (but not the password itself).

If Chrome suspects that your settings have been tampered with, Chrome reports the URL of the last downloaded potentially dangerous file, and information about the nature of the possible tampering, to the Safe Browsing service.

For some downloads, Chrome may ask you to opt in to reporting to Google Safe Browsing some data relevant to

security, in order to improve the quality of download protection. Once you've opted in, some downloaded files that are suspicious will be sent to Google for investigation each time they are encountered. You can change this opt-in setting at any time in the Chrome settings.

Chrome asks your permission before using certain web features (APIs) that might have associated risks. To improve the safety and utility of Chrome permissions, Chrome may anonymously report the domains on which you grant, reject and revoke permissions or ignore or dismiss permission prompts. This happens only if you are a Safe Browsing user and have activated syncing your browsing history and settings with Google without a custom passphrase.

For all Safe Browsing requests and reports, Google logs the transferred data in its raw form and retains this data for up to 30 days. Google collects standard log information for Safe Browsing requests, including an IP address and one or more cookies. After at most 30 days, Safe Browsing deletes the raw logs, storing only calculated data in an anonymized form that does not include your IP addresses or cookies. Additionally, Safe Browsing requests won't be associated with your Google Account. They are, however, tied to the other Safe Browsing requests made from the same device.

Unwanted software protection

The Windows version of Chrome is able to detect and remove certain types of software that violate [Google's Unwanted Software Policy](#). If left in your system, this software may perform unwanted actions, such as changing your Chrome settings without your approval. Chrome periodically scans your device to detect potentially unwanted software. In addition, [if you have opted in to automatically report details of possible security incidents to Google](#), Chrome will report information about unwanted software, including relevant file metadata and system settings linked to the unwanted software found on your computer.

If you perform an unwanted software check on your computer from the Settings page, Chrome reports information about unwanted software and your system. System information includes metadata about programs installed or running on your system that could be associated with harmful software, such as: services and processes, scheduled tasks, system registry values commonly used by malicious software, command-line arguments of Chrome shortcuts, Windows proxy settings, and software modules loaded into Chrome or the network stack. You can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the scan.

If unwanted software is detected, Chrome will offer you an option to clean it up by using the Chrome Cleanup Tool. This will [quarantine](#) detected malicious files, delete harmful extensions and registry keys, and [reset](#) your settings. The Chrome Cleanup Tool also reports information about unwanted software and your system to Google, and again you can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the cleanup.

This data is used for the purpose of improving Google's ability to detect unwanted software and offer better protection to Chrome users. It is used in accordance with Google's [Privacy Policy](#) and is stored for up to 14 days, after which only aggregated statistics are retained.

Navigation error tips

Google Chrome can show tips to help guide you to the page you were trying to reach in cases where the web address cannot be found, a connection cannot be made, the server returns a very short (under 512 byte) error message, or you've navigated to a parked domain.

Google Chrome will first check the address against a locally-stored list of suspected parked domains. If there is a match, Chrome sends a partial fingerprint (a hash prefix) of the URL to Google for verification that the domain is indeed parked. This uses the same methodology as the Safe Browsing service (see the "Safe Browsing protection" section, above).

In the case of other navigation errors, the URL of the web page you're trying to reach is stripped of all GET parameters, and then sent to Google in order to retrieve navigation tips. This information is logged and anonymized in the same manner as [Google web searches](#). The logs are used to ensure and improve the quality of the feature.

Additionally, to provide you with more informative error messages when a domain name cannot be found, Chrome will investigate the underlying cause by attempting to resolve "google.com" using both [Google Public DNS](#) and the default DNS service configured for your system.

In the event that Chrome detects SSL connection timeouts, certificate errors, or other network issues that might be caused by a captive portal (a hotel's WiFi network, for instance), Chrome will make a cookieless request to https://www.gstatic.com/generate_204 and check the response code. If that request is redirected, Chrome will open the redirect target in a new tab on the assumption that it's a login page. Requests to the captive portal detection page are not logged.

You can [disable navigation error tips](#) by unchecking the box in the "Privacy" section of Google Chrome's options.

Offline Indicator

On Android versions Lollipop and older, when Chrome detects a network change, it sends a cookieless request to http://connectivitycheck.gstatic.com/generate_204 or http://clients4.google.com/generate_204 to determine whether you're offline and display an offline indicator.

Software updates

Desktop versions of Chrome and the Google Chrome Apps Launcher use Google Update to keep you up to date with the latest and most secure versions of software. In order to provide greater transparency and to make the technology available to other applications, the Google Update technology is open source.

Google Update requests include information necessary for the update process, such as the version of Chrome, its release channel, basic hardware information, and update errors that have been encountered. The update requests also send Google information that helps us understand how many people are using Google Chrome and the Chrome Apps Launcher – specifically, whether the software was used in the last day, the number of days since the last time it was used, the total number of days it has been installed, and the number of active profiles. Google Update also periodically sends a non-unique four-letter tag that contains information about how you obtained Google Chrome. This tag is not personally identifiable, does not encode any information about when you obtained Google Chrome, and is the same as everyone who obtained Google Chrome the same way.

Because Chrome OS updates the entire OS stack, Google Update on Chrome OS also sends the current Chrome OS version and hardware model information to Google in order to ensure that the correct software updates and hardware manufacturer customizations such as apps, wallpaper, and help articles are delivered. This information is not personally identifiable, and is common to all users of Chrome OS on the same revision of device.

Unlike the desktop versions of Chrome, the delivery and management of updates for mobile versions of Chrome are managed through the app stores for Android and iOS. Mobile versions of Chrome utilize the servers described above for counting active installations.

Chrome extensions and applications that you've installed are kept up to date with a similar system used for updating desktop versions of Chrome. These update requests include similar information (such as the application ID, when the application was last used, and how long it's been installed). We use these requests to determine the aggregate popularity and usage of applications and extensions. If you are using an extension or application restricted to a certain audience, authentication tokens are sent with the update requests for these add-ons. For security reasons, Chrome also occasionally sends a cookieless request to the Chrome Web Store, in order to verify that installed extensions and applications that claim to be from the store are genuine.

In order to keep updates as small as possible, Google Chrome is internally split into a variety of components, each of which can be updated independently. Each component is uniquely identified via an ID that is shared among all Google Chrome installations (e.g., "fmeadaodfnidclnjhlkdjgkolmhmfofk"). An update request for a component contains this ID, the hash of the previous download (called a "fingerprint"), and the component's version. Because every installation has the same ID, and downloads of the same component have the same fingerprint, none of this information is personally identifiable.

If you install web apps on an Android device, a Google server is responsible for creating a native Android package that can be verified for authenticity by Chrome. When Chrome is updated or notices that the web app's manifest has changed, Chrome asks the server for a new version of the Android package in a cookieless request. If the information needed to create the native Android package cannot be acquired by the server (e.g., because the information is behind a corporate firewall), Chrome sends it to Google and an Android package is created that is unique to you. It contains a unique and random identifier that is not tied to your identity.

Chrome may also download and run a binary executable (e.g., as part of the software update or to improve Safe Browsing protection). These executables are cryptographically signed and verified before execution. Chrome may download further static resources like dictionaries on demand to reduce the size of the installer.

On Windows and OS X versions of Chrome, the recovery component tries to repair Google Update when it's broken. After the relevant binary is executed, Google Update uploads statistics on the actions that were performed. These statistics contain no personally identifiable information.

Network time

On desktop platforms, Chrome uses network time to verify SSL certificates, which are valid only for a specified time. At random intervals or when Chrome encounters an expired SSL certificate, Chrome may send requests to Google to obtain the time from a trusted source. These requests are more frequent if Chrome believes the system clock is inaccurate. These requests contain no cookies and are not logged on the server.

Counting installations

In order to measure the success rate of Google Chrome downloads and installations of the Windows version of Google Chrome, a randomly-generated token is included with Google Chrome's installer. This token is sent to Google during the installation process to confirm the success of that particular installation. A new token is generated for every install. It is not associated with any personal information, and is deleted once Google Chrome runs and checks for updates the first time.

For Chrome to know how many active installations it has, the mobile version of Chrome sends a ping to Google with a salted hash of a device identifier on an ongoing basis. The desktop version of Chrome does not send any stable identifier to count active installations. Instead an anonymous message to Google with a timestamp of the last ping is used to infer number of active installations.

Measuring effectiveness of a promotion

Chrome utilizes two measurements to understand how effective a promotional campaign has been: how many Chrome

To measure installations or reactivations of Chrome through a campaign, Chrome will send a token or an identifier unique to your device to Google at the first launch of Chrome, as well as the first search using Google. On desktop versions of Chrome, a token unique to your device is generated. The same token will be sent if Chrome is later reinstalled at first launch and at first use of the Omnibox after reinstallation or reactivation. Rather than storing the token on the computer, it is generated when necessary by using built-in system information that is scrambled in an irreversible manner. On iOS, Chrome uses the IDFA for counting installations acquired by a campaign, and it can be reset in iOS settings.

To measure searches and Chrome usage driven by a particular campaign, Chrome inserts a promotional tag, not unique to you or your device, in the searches you perform on Google. This non-unique tag contains information about how Chrome was obtained, the week when Chrome was installed, and the week when the first search was performed. For desktop versions of Chrome, Chrome generates a promotional tag, if the promotional installation token described in the previous paragraph indicates that Chrome has been installed or reactivated by a campaign on a device which has not been associated with any campaign yet. For Chrome on Mobile, a promotional tag is always sent regardless of the source of installations.

The promotional tag is generated using a software library called "RLZ" and looks similar to "1T4ADBR_enUS236US239". The RLZ library was fully open-sourced in June 2010. For more information, please see the In the Open, for RLZ post on the Chromium blog and the article "How To Read An RLZ String". On Android, this promotional tag can also be a readable string like "android-hms-tmobile-us" instead of an RLZ string, and is not unique to either you or your device.

This non-unique promotional tag is included when performing searches via Google (the tag appears as a parameter beginning with "rlz=" when triggered from the Omnibox, or as an "x-rlz-string" HTTP header). We use this information to measure the searches and Chrome usage driven by a particular promotion.



If usage statistics and crash reports are enabled, the RLZ string is sent along with the report. This allows us to improve Chrome based on variations that are limited to specific geographic regions.

For the desktop version of Chrome, you can opt-out of sending this data to Google by uninstalling Chrome, and installing a version downloaded directly from www.google.com/chrome. To opt-out of sending the RLZ string in Chrome OS, press Ctrl + Alt + T to open the crosh shell, type rlz disable followed by the enter key, and then reboot your device.

Usage statistics and crash reports

Chrome has a feature to automatically send usage statistics and crash reports to Google in order to help improve Chrome's feature set and stability.



Usage statistics contain information such as system information, preferences, user interface feature usage, responsiveness, and memory usage. This feature is enabled by default for Chrome installations of version 54 or later. You can enable or disable the feature in the "Privacy" section of Google Chrome's settings. These statistics do not include any personal information. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs or personal information depending on what was happening at the time of the crash.

When this feature is enabled, Google Chrome stores a randomly generated unique token on your device, which is sent to Google along with your usage statistics and crash reports. The token does not contain any personal information and is used to de-duplicate reports and maintain accuracy in statistics. This token is deleted when the feature is disabled and a new token is regenerated when the feature is enabled again.

Along with usage statistics and crash reports, Chrome also reports anonymous, randomized data that is constructed in a manner which is not linked to the unique token, and which ensures that no information can be inferred about any particular user's activity. This data collection mechanism is summarized on the Google research blog, and full technical details have been published in a technical report and presented at the 2014 ACM Computer and Communications Security conference.

Chrome will also anonymously report to Google if requests to websites operated by Google fail or succeed in order to detect and fix problems quickly.

If you are also syncing your browsing history without a sync passphrase, Chrome usage statistics include information about the web pages you visit and your usage of them. The information will also include the URLs and statistics related to downloaded files. If you sync extensions, these statistics will also include information about the extensions that have been installed from Chrome Web Store. The URLs and statistics are sent along with a unique device identifier that can be reset by turning off history Sync or usage statistics and crash reports. The usage statistics are not tied to your Google account. Google only stores usage statistics associated with published extensions, and URLs that are known by Google's web crawlers. We use this information to improve our products and services, for example, by identifying web pages which load slowly; this gives us insight into how to best improve overall Chrome performance. We also make some statistics available externally, through efforts like the Chrome User Experience Report. Externally published reports are conducted in highly aggregated manner to not reveal individual user's identity.

On iOS, if you are syncing your browsing history without a sync passphrase, Chrome reports usage for certain URLs that other Google apps could open. For example, when you tap on an email address, Chrome presents a dialog that allows you to choose between opening with Google Gmail or other mail apps installed on your device. The usage information also includes which apps were presented to you, which one was selected, and if a Google app was installed. Chrome does not log the actual URL tapped. If you are signed in, this usage is tied to your Google account. If you are signed out, the information is sent to Google with a unique device identifier that can be regenerated by resetting the Google Usage ID found in Chrome settings. The raw reports are deleted within 60 days, after which only the aggregated statistics remain.

Google Surveys in Chrome

When you have "send usage statistics" enabled, you may be randomly selected to participate in surveys to evaluate consumer satisfaction with Chrome features. If you are selected, Chrome on Android requests a survey from Google for you. If a survey is available, Chrome then asks you to answer the survey and submit the responses to Google.

The survey also records basic metrics about your actions, such as time spent looking at the survey and elements that the user clicked. These metrics are sent to Google even if you do not fully complete the survey.

To ensure that surveys are spread evenly across users and not repeatedly served to a single user, the feature stores a randomly generated unique token on the device. This token is used solely for the survey requests and does not contain any personal information. If you disable sending usage statistics, the token will be cleared.

Suggestions for spelling errors

Desktop versions of Chrome can provide smarter spell-checking by sending text you type into the browser to Google's servers, allowing you to apply the same spell-checking technology that's used by Google products like Docs. If this feature is enabled, Chrome sends the entire contents of text fields as you type in them to Google, along with the browser's default language. Google returns a list of suggested spellings that are displayed in the context menu. Cookies are not sent along with these requests. Requests are logged temporarily and anonymously for debugging and quality improvement purposes.

This feature is disabled by default; to turn it on, click "Ask Google for suggestions" in the context menu that appears when you right-click on a misspelled word. You can also turn this feature on or off with the "Use a web service to help resolve spelling errors" checkbox in the Privacy section of Chrome settings. When the feature is turned off, spelling suggestions are generated locally without sending data to Google's servers.

Mobile versions of Chrome rely on the operating system to provide spell-checking.

Translate

Google Chrome's built-in translation feature helps you read more of the Web, regardless of the language of the web page. The feature is enabled by default.



Translation can be disabled at any time in Chrome's settings.

Language *detection* is done entirely using a client-side library, and does not involve any Google servers. For *translation*, the contents of a web page are only sent to Google if you explicitly decide to translate it by clicking "Translate" on the bar, or if you've previously chosen "Always translate" for a given language via the translate bar Options menu.

If you do choose to translate a web page, the text of that page is sent to Google Translate for translation. Your cookies are not sent along with that request and the request is sent over SSL. This communication with Google's translation service is covered by the Google privacy policy.

If you've chosen to sync your Chrome history, statistics about the languages of pages you visit and about your interactions with the translation feature will be sent to Google to improve Chrome's understanding of the languages you speak and when Chrome should offer to translate text for you.

Sign In to Chrome and sync

You have the option to use the Chrome browser while signed in to your Google Account, with or without sync enabled.

On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. If you are signed in to Chrome, Chrome may offer to save your payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can turn off Chrome sign-in.

When you're signed-in and have enabled sync with your Google Account, your personal browsing data information is saved in your Google Account so you may access it when you sign in and sync to Chrome on other computers and devices. Synced data can include bookmarks, saved passwords, open tabs, browsing history, extensions, addresses, phone numbers, payment methods, and more. In advanced sync settings, you can choose which types of data to synchronize with this device. By default, all syncable data types are enabled. You can turn sync on or off in the "People" section of Chrome settings.

If you have turned on sync and signed out of the account you are syncing to, sync will pause sending all syncable data to Google until you sign back in with the same account. Some sync data types (such as bookmarks and passwords) that are saved locally while sync is paused will automatically be synced to your account after you sign back in with the same account.

On mobile versions of Chrome, you can sign into or sign out of Chrome from Chrome settings. Signing into Chrome will also turn on sync. This can be done for any account that has already been added to the mobile device without authenticating again.

On both desktop and mobile, signing into Chrome keeps you signed into Google web services until you sign out of Chrome. On mobile, signing into Chrome will keep you signed in with all Google Accounts that have been added to the device. On desktop, it will keep you signed in with all Google Accounts that you added from a Google web service, unless you have set “Keep local data only until you quit your browser” in your [cookie settings](#).

On Android and desktop, Chrome signals to Google web services that you are signed into Chrome by attaching an X-Chrome-Connected and/or C-Chrome-ID-Consistency-Request header to any HTTPS requests to Google-owned domains. On iOS, the CHROME_CONNECTED cookie is used instead. This allows those Google web services to update their UI accordingly. If you are using a managed device, your system admin may disable the sign in feature or require that data be deleted when you disconnect your account.

Google uses your personal synchronized data to provide you a consistent browsing experience across your devices, and to customize features in Chrome. You can manage your synchronized history by going to [chrome://history](#) in your Chrome browser. If “Include history from Chrome and other apps in your Web & App Activity” is checked on the [Web & App Activity](#) controls page, Google also uses your synchronized browsing data to provide personalized Google products and services to you. You can change your preference any time, and manage individual [activities associated with your Google account](#).

The paragraph above describes the use of your personal browsing history. Google also uses aggregated and anonymized synchronized browsing data to improve other Google products and services. For example, we use this information to improve Google Search by helping to detect mobile friendly pages, pages which have stopped serving content, and downloads of malware.

If you would like to use Google's cloud to store and sync your Chrome data without allowing any personalized and aggregated use by Google as described in the previous paragraphs, you can choose to encrypt all of your synced data with a [sync passphrase](#). If you choose this option, it's important to note that Google won't have access to the sync passphrase you set; we won't be able to help you recover data if you forget the passphrase. Regardless of how you choose to encrypt your data, all data is always sent over secure SSL connections to Google's servers.

If you're signed into Chrome and are syncing passwords and/or other types of login credentials without a sync passphrase, these credentials are stored in your Google Account. Chrome may help you sign in with credentials you've saved in Android apps on websites that are associated with the respective apps. Likewise, credentials you've saved for websites can be used to help you sign into related Android apps. You can view the credentials you've saved in Chrome and Android by visiting [passwords.google.com](#) in any browser. If you've saved credentials for Android applications, Chrome periodically sends a cookieless request to Google to get an updated list of websites that are associated with those applications. To stop websites and Android apps from automatically signing in using credentials you previously saved, you can turn off Auto Sign-In on [passwords.google.com](#) or in Chrome settings under “Manage passwords”. For more details see [this article](#).

If you sync your browsing history without a sync passphrase and your browser's usage statistics and crash reports setting is also enabled, your usage statistics and crash reports will include statistics about the pages you visit. You can read more in the [Usage statistics and crash reports](#) section of this Whitepaper.

All data synchronized through Google's servers is subject to [Google's Privacy Policy](#). To get an overview of the Chrome data stored for your Google Account, go to the [Chrome section of Google Dashboard](#). That page also allows you to stop synchronization completely and delete all sync data from Google's servers.

Autofill and Password Management

Google Chrome has a [form autofill feature](#) that helps you fill out forms on the web more quickly. Autofill is enabled by default, but it can be turned off at any time in Chrome's settings.

If Autofill is enabled and you encounter a web page containing a form, Chrome sends some information about that form to Google. This information includes a hash of the web page's hostname, as well as form identifiers (such as field names), and the basic structure of the form. In response, Chrome receives a prediction of each field's data type (for example, “field X is a phone number, and field Y is a country”). This information helps Chrome match up your locally stored Autofill data with the fields of the form.

If Autofill is enabled when you *submit* a form, Chrome sends Google some information about the form along with the types of data you submitted. This information includes a hash of the web page's hostname, as well as form identifiers (such as field names), the basic structure of the form, and the observed data types for the fields (i.e., field X was a phone number, field Y was a country). The values you entered into the form are not sent to Google. This information helps Chrome improve the quality of its form-filling over time.

You can manage your Autofill entries via [Chrome's settings](#), and you can edit or delete saved information at any time. Chrome will never store full credit card information (card number, cardholder name, and expiration date) without explicit confirmation. In order to prevent offering to save cards you have shown disinterest in saving, Chrome stores the

Chrome may help you sign in to websites with credentials you've saved to Chrome's password manager or Google Smart Lock by autofilling sign-in forms, by offering you an account picker, or by automatically signing you in. You can manage and delete your saved credentials in the "Forms and passwords" section of Chrome's settings. If you enable password management, the same kind of data about forms as described above is sent to Google to interpret password forms correctly and enable Chrome to offer password generation that meets site-specific requirements.

Also, if you choose, you can bring your Autofill data with you to all your Chrome-enabled devices by syncing it as part of your browser settings (see the "Sign In to Chrome" section of this document). If you choose to sync Autofill information, field values are sent as described in "Sign In to Chrome"; otherwise, field values are not sent.

Payments

When you're signed into Chrome with your Google Account, Chrome may offer to save payment cards and related billing addresses into payment data under the same Google account, and include cards from your account among the autofill suggestions on payment web forms. Integration with Google Payments can be disabled via Chrome's Advanced sync settings. If integration with Google Payments is disabled, credit cards will be saved locally but will not be synced. If integration with Google Payments is enabled, Chrome may offer to autofill forms with credit card data stored in your Google Payments account. The cards from your Google Payments account not already saved locally are masked until you provide the correct CVV code. When providing your CVV code for verification, you can choose to store the credit card locally as part of your Chrome Autofill data. If you choose not to store the card locally, you will be prompted for your CVV code each time you use the card. If you use a card from Google Payments, Chrome will collect information about your computer and share it with Google Payments to prevent fraudulent use of your card.

To delete credit card information saved in Chrome, follow the "Add and edit credit cards" steps in the Autofill article. When you delete a credit card that's also saved in your Google Payments account, you will be redirected to the Google Payments to complete the deletion. After your card has been deleted from your Google Payments account, Chrome will automatically remove that card from your Autofill suggestions.

To save a card locally on the device only, while still being signed in to Chrome with a Google Account, you can add a card from the "Add" button in the "Payment methods" section in Chrome settings. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can turn off Chrome sign-in. If you have sync turned on, you can disable syncing payment methods and addresses to Google Pay under "Sync" in Chrome settings. You can also turn the Payments Autofill feature off altogether in settings.

Chrome also supports the PaymentRequest API by allowing you to pay for purchases with credit cards from Autofill, Google Payments, and other payment apps already installed on your device. Google Payments and other payment apps are only available on an Android device. PaymentRequest allows the merchant to request the following information: full name, shipping address, billing address, phone number, email, credit card number, credit card expiration, CVV, and Google Payments credentials. Information is not shared with the merchant until you agree.

Geolocation

Google Chrome supports the Geolocation API, which provides access to fine-grained user location information with your consent.

By default, Chrome will request your permission when a web page asks for your location information, and does not send any location information to the web page unless you explicitly consent.

Furthermore, whenever you are on a web page which is using your location information, Chrome will display a location icon on the right side of the omnibox. You can click on this icon in order to find out more information or manage location settings.



In Chrome's settings, by clicking "Show advanced settings.", then clicking "Content Settings" and scrolling to the "Location" section, you can choose to allow all sites to receive your location information, have Chrome ask you every time (the default), or block all sites from receiving your location information. You can also configure exceptions for specific web sites.

In the Android version of Chrome, your default search engine automatically receives your location when you conduct a search. On the iOS version of Chrome, by default your location is sent to Google if you conduct a search from the omnibox. Read more about how your default search engine handles geolocation and how to manage your settings in the Omnibox section of the whitepaper.

If you do choose to share your location with a web site, Chrome will send local network information to Google (also used by other browsers such as Mozilla Firefox) in order to estimate your location. This local network information can include data about nearby Wi-Fi access points or cellular signal sites/towers (even if you're not using them), and your computer's IP address. The requests are logged, and aggregated and anonymized before being used to operate, support, and improve the overall quality of Google Chrome and Google Location Services.

For further reading on the privacy and user interface implications of the Geolocation API (as well as other HTML5 APIs), see "Practical Privacy Concerns in a Real World Browser" written by two Google Chrome team members.

Speech to text

Chrome supports the Web Speech API, a mechanism for converting speech to text on a web page. It uses Google's servers to perform the conversion. Using the feature sends an audio recording to Google (audio data is not sent directly to the page itself), along with the domain of the website using the API, your default browser language and the language settings of the website. Cookies are not sent along with these requests.

Google Assistant "Ok Google"

The Google Assistant feature is integrated into some models of Chrome OS devices. If you opt in to the feature, Chrome OS listens for you to say "Ok Google" and sends the audio of the next thing you say, plus a few seconds before, to Google. Detection of the phrase "Ok Google" is performed locally on your computer, and the audio is only sent to Google after it detects "Ok Google". You can enable or disable this feature in Google Assistant Settings.

Enabling this feature in Chrome Settings will cause Chrome to listen whenever the screen is unlocked. On Chrome OS devices with a local audio processor, the device also listens when the device is asleep. On these devices, The Google Assistant feature only works if Voice & Audio Activity is enabled for your Google account. Chrome will prompt you to enable Voice & Audio Activity for the associated Google account if it is disabled.

Once the audio has been converted to text, a search with that text is submitted to Google. If you have used the "Ok Google" search before on a device but turned off Voice & Audio Activity later, your device is still capable of processing your voice and sending the audio to Google but the voice is deleted shortly.

You can determine your Chrome OS device's behavior by examining the text in the "Search and Assistant" section of settings.

Google Cloud Print

The Google Cloud Print feature allows you to print documents from your browser over the Internet. You do not need a direct connection between the machine that executes Chrome and your printer.

If you choose to print a web page via Cloud Print, Chrome will generate a PDF of this website and upload it over an encrypted network connection to Google's servers. If you choose to print other kinds of documents, they may be uploaded as raw documents to Google's servers.

A print job will be downloaded by either a Chrome browser ("Connector") or a Cloud Print capable printer that you selected when printing the website. In some cases the print job must be submitted to a third-party service to print (HP's ePrint, for example).

The print job is deleted from Google's servers when any of three criteria is met:

- You delete the print job
- The job has been printed and marked as printed by the printer/connector
- The job has been queued on Google's servers for 30 days

You can manage your printers and print jobs on the Google Cloud Print website.

SSL certificate reporting

Chrome stores locally a list of expected SSL certificate information for a variety of high-value websites, in an effort to prevent man-in-the-middle attacks. For Google websites and other websites that choose to opt in, Chrome will report a possible attack or misconfiguration. If the certificate provided by the web server doesn't match the expected signature, Chrome reports information about the SSL certificate chain to Google or to a report collection endpoint of the website's choosing. Chrome sends these reports only for certificate chains that use a public root of trust.

You can enable this feature by opting in to report data relevant to security, as described in the Safe Browsing section. While you are opted in, two kinds of reports may be sent to Google's security team. Each time you see an SSL error page, a report will be sent containing the SSL certificate chain, the server's hostname, the local time, and relevant details about the validation error and SSL error page type. Additionally, each time a mismatch between different certificate verifiers is detected, a report will be sent containing the certificate chain and the verification result.

Because Chrome sends these reports for all certificate chains, even those that chain to a private root of trust, these chains can contain personally identifiable information. You can opt out anytime by unchecking the box "Help Improve Safe Browsing" in the Privacy section of Chrome's advanced settings.

The SSL certificate reporting feature is not available on Chrome iOS.

Installed Applications and Extensions

Users can install external apps and extensions for the desktop versions of Chrome to add features to or customize their Chrome browsers. Installing an application or extension from the Chrome Web Store directly or via an inline installation flow on a third-party site involves a request to the Chrome Web Store for details about the application. This request includes cookies, and if you're logged into Google when you install an application, that installation is recorded as part of your Google account. The store uses this information to recommend applications to you in the future, and in aggregate to evaluate application popularity and usage. As noted above, applications and extensions are updated via Google

As they're more deeply integrated into Chrome, applications and extensions that you choose to install can request access to additional capabilities, enabling functionality that doesn't make sense on the web at large: background notifications or raw socket access, for instance. These additional permissions may change the way your data is collected and shared, as extensions and applications might have access to data regarding the websites you visit, and might be capable of monitoring or modifying your interactions with the web. When installing an application or extension, Chrome may first warn you about certain capabilities. Please do take the time to read and evaluate this warning before proceeding with the installation. Note also that interactions with and data collected by these third-party applications and extensions are governed by their own privacy policies, not Google's privacy policy.

Push messaging

Your device may receive push messages from the backend servers of apps and extensions installed in Chrome, websites that you grant the "notification" permission to, and your default search engine. Disabling push messages from your default search engine is done in the same way as disabling push messages from any site, by visiting the "Notifications" section of "Site settings".

Push message data is sent over a secure channel from the developer through Google's infrastructure to Chrome on your device, which can wake up apps, extensions, and websites (including your default search engine) to deliver the message. The developer may end-to-end encrypt the message data, or may send it in a form such that Google servers process it as plain text. Google servers retain up to 4 weeks' worth of messages to ensure delivery to users even if their devices are offline at the time of the initial pushing.

If the notification permission is set to "granted" for any website (including the default search engine), or you have an app or extension installed that uses push messaging, then Chrome provides the app's, extension's, or website's server with one or more registration tokens that can be used to send messages to the entity (app, extension, or website). Websites you visit in Incognito mode are not allowed to send you push messages and therefore cannot get a registration token.

When you uninstall an app or extension, revoke the notification permission for a website, or clear cookies for a permitted website, its registration token is revoked and will not be reused, even if the same app or extension is re-installed or the same website is re-visited. Registration tokens used by Chrome components such as Sync are revoked once they are no longer in use (for example, when the user disables Sync). When a registration token is revoked, the associated entity on your device stops receiving messages sent from its developer's server.

The registration tokens that are passed to entities contain an encrypted device ID, which is used for routing the messages. Google can decrypt the device ID, but other entities cannot, and the encryption is designed so that two registration tokens for the same device ID cannot be correlated. On desktop versions of Chrome, the device ID is reset when the Chrome profile is removed (via the "People" section in Chrome's Settings), or when neither Chrome Sync nor any of the entities requires it for push messaging. On Android, the lifetime of the device ID is governed by the operating system and is independent of Chrome. Any messages routed to registration tokens containing a revoked device ID will not be delivered.

Chrome custom tabs

On Android devices, an app developer may use a Custom Tab to show web content when you click on a URL from their app. A Custom Tab may look different from a regular Chrome tab, for example it may have app-specified visual style, and the absence of an editable URL bar. Despite the different visual style a Custom Tab may have, the data sent and received in the Custom Tab, such as cookies, saved passwords and browsing history function the same way they do in a normal Chrome tab. The Custom Tab is an app-customized view using the same underlying user profile.

With Chrome Custom Tabs, an Android app developer may also specify custom actions in the Chrome toolbar and overflow menu that are relevant to their app, for example, "share", "save page", "copy URL". If you tap on such a button, the address of the current website is shared with the application.

An application can request Chrome to pre-render a given URL in the background. This allows Chrome to show you a pre-loaded site instantly when you open it from the app. At the same time it allows an application to set cookies in your browser in the background. To disable pre-rendering, you can uncheck "Prefetch page resources" in the privacy settings.

Trusted Web Activities are a form of Chrome Custom Tab where the top bar is not present, allowing web browsing with no browser UI but with access to the cookie jar. They can only be used to view web content on an origin that the client app can prove that it owns using Digital Asset Links. If the user navigates off this origin the the top bar reappears.

When the client app is uninstalled or has its data cleared through Android Settings, Chrome will allow the user to clear data for the linked origin.

Continue where you left off

If you have selected the option to "Continue where you left off" in settings on desktop versions of Chrome, when you open Chrome, it attempts to bring you right back to the way things were when the browser was closed. Chrome reloads the tabs you had open and persists session information to get you up and running as quickly as possible. This feature effectively extends a browsing session across restarts. In this mode, session cookies are no longer deleted when the browser closes; instead, they remain available on restart to keep you logged into your favorite sites.

On OS X, when you restart your device, a checkbox in the OS confirmation dialog asks you whether you want to re-open applications and windows after restart. If you check this box, Chrome restores tabs and windows, as well as the session cookies, even if you have disabled "Continue where you left off" on Chrome.

On mobile versions of Chrome, this feature is always enabled without a setting.

Chrome Variations

We want to build features that users want, so a subset of users may get a sneak peek at new functionality being tested before it's launched to the world at large. A list of field trials that are currently active on your installation of Chrome will be included in all requests sent to Google. This Chrome-Variations header (X-Client-Data) will not contain any personally identifiable information, and will only describe the state of the installation of Chrome itself, including active variations, as well as server-side experiments that may affect the installation.

The variations active for a given installation are determined by a seed number which is randomly selected on first run. If usage statistics and crash reports are disabled, this number is chosen between 0 and 7999 (13 bits of entropy). If you would like to reset your variations seed, run Chrome with the command line flag "--reset-variation-state". Experiments may be further limited by country (determined by your IP address), operating system, Chrome version and other parameters.

Do Not Track

If you enable the "Do Not Track" preference in Chrome's settings, Chrome will send a DNT:1 HTTP header with your outgoing HTTP, HTTPS and SPDY browsing traffic (Chrome cannot, however, guarantee that NPAPI plugins also send the header.) The header will not be sent with system traffic such as the geolocation, metrics or device management services.

The effect of Do Not Track depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example, to improve security; to provide content, services, ads and recommendations on their websites; and to generate reporting statistics.

Chrome on iOS now uses WKWebView to provide a more stable and faster browser. As a result of this move, the Do Not Track preference is no longer available due to iOS constraints. If Apple makes changes to allow this feature, Chrome will make Do Not Track available again in iOS.

Plugins

Chrome ships with an Adobe Flash Player implementation that is based on the Pepper API. Flash and other Pepper-based plugins may ask you for "Access to your computer". If you grant this permission, the plugin is granted unsandboxed access. This allows content providers to offer you access to DRM protected content like videos or music but may have security and privacy implications, so consider carefully whether you trust a plugin or website with this privilege.

Media licenses

Some websites encrypt media to protect against unauthorized access and copying. When users play media from these sites, they typically log into the site, which authenticates the user, and then digital rights management negotiates a key exchange for the decryption and playback of the media.

For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. The implementation of that API is tightly coupled with the browser to protect user privacy and security, through Content Decryption Modules (CDM), which are provided by digital rights management solutions such as Google Widevine or Microsoft PlayReady.

When a user asks Chrome to play encrypted HTML5 media (for example, watching a movie on Google Play Movies), Chrome will generate a request for a license to decrypt that media. This license request contains an automatically generated request ID, which is created by the Content Decryption Module, as well as proof that the CDM is legitimate. After generation, the license request is typically sent to a license server managed by either the content website or Google. Neither the license request, the proof, nor the request ID include any personally identifying information. After being sent, the license request is not stored locally on the user's device.

As part of the license request, Chrome also generates a unique session ID which does not contain personally identifying information. This session ID is sent to the license server, and when the server returns a license the session ID is used to decrypt the media. The session ID may be stored locally even after the site has been closed. The license may also be stored locally for offline consumption of protected content. Session ID and licenses may be cleared by the user in Chrome using [Clear Browsing Data](#) with "Media licenses" enabled.

When returning a license, the site license server may include a client ID, generated by the site. This client ID is unique to the user and the site, it is not shared between sites. If provided, the client ID is stored locally and included by Chrome in subsequent license requests to that site. The client ID may be cleared by the user in Chrome using [Clear Browsing Data](#) with "Media licenses" enabled.

On some platforms, the website may additionally request verification that the device is eligible to play specific types of protected content; on Chrome OS, this is known as Verified Access). In this case, Google creates a certificate using a unique hardware identifier for the device. This hardware ID identifies the device, but does not identify the user. If the user agrees, Google receives the hardware ID and generates a certificate verifying the device for the requested site. The certificate does not include the hardware ID or any other information that could permanently identify the device. Certificates are stored locally similar to other cached browsing data, and may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Media licenses” enabled.

Some sites use Flash instead of HTML5. If a website you visit chooses to use Adobe Flash Access DRM protection, Chrome for Windows and Chrome OS will give Adobe Flash access to a device identifier. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with “Media licenses” enabled.

In order to give you access to licensed music, the [Google Play Music app](#) can retrieve a device identifier that is derived from your hard drive partitions or, on a Chrome OS or Linux installation, from a unique file on your disk. This identifier can be reset by reinstalling your operating system.

Cloud policy

When you sign into a Chrome OS device, Chrome on Android, or a desktop Chrome profile with an account associated with a Google Apps domain, Chrome checks whether the domain has configured enterprise policies. If so, the Chrome OS user session or Chrome profile is assigned a unique ID, and registered as belonging to that domain. Any configured policies are applied to the profile. In order to revoke the registration, you'll need to remove the Chrome OS user profile, sign out of Chrome on Android, or remove the desktop profile.

Additionally, Chrome OS devices can be enrolled to a Google Apps domain by a domain admin. This will enforce enterprise policies for the entire device, such as providing shared network configurations and restricting access to developer mode. When a Chrome OS device is enrolled to a domain, then a unique device ID is registered to the device. In order to revoke the registration, the admin will need to wipe the entire Chrome OS device.

Registered profiles and devices check for policy changes periodically (every 3 hours by default). In some cases, the server pushes policy changes to the client without waiting for Chrome's periodic check. Unregistered profiles check whether a policy has been turned on for their domain each time Chrome starts up.

The [policy list](#) contains details about the types of configurations that are available via Cloud Policy.

Data Saver

If you enable Data Saver, Chrome will send your traffic through Google's optimizing proxy servers. This option reduces the amount of data downloaded and speeds up your page loads.

Most of the time, only your HTTP traffic is transparently proxied, and you won't notice any changes to the page. However, if Chrome anticipates the page will load especially slowly, both HTTP and HTTPS pages will be optimized to load only the essential content. For HTTPS origins, the transcoded pages are served from a Google-owned domain instead of being transparently proxied. Because these pages are served from a Google-owned domain instead of the original domain, Chrome will not send any origin-scoped information (e.g., cookies or data from local storage) for the original domain to Google, and Google cannot set any origin-scoped information for the original domain in Chrome. Pages loaded in Incognito are never proxied or optimized by Data Saver.

Request URLs are logged, but Cookie and If-None-Match headers are stripped from the logs (and cookies are never seen in the case of HTTPS pages). Additionally, the content of proxied pages is cached but not logged. The logs are not associated with your Google Account, and the entire log entry is removed within 14 days. These logs are also governed by standard Google search logging policies.

Google uses the logged and cached data to improve both Data Saver and Safe Browsing; for example, more effective optimizations can be uncovered by analyzing timing data for pages loaded through the proxy service, and malware can be detected more rapidly by analyzing response data in realtime.

Your IP address is forwarded to the origin HTTP server via an X-Forwarded-For header, in accordance with the HTTP standard. The Data Saver service is a transparent proxy, *not* an anonymization service.

By default, the connection between the browser and the Data Saver proxy is over an encrypted channel. However, a network administrator can [disable](#) the use of an encrypted channel to Data Saver.

Supervised Users

If you create a supervised user on Chrome or Chrome OS, certain information such as the supervised user's browsing activity, profile settings and permissions requests for blocked content will be sent to Google in association with your Google Account. You can access the browsing activity of your supervised users at [chrome.com/manage](#). In order to remove data that is associated with a supervised user from Google's servers, please sign in to your Google Account at [chrome.com/manage](#) and delete the respective supervised user.

Using Chrome with a kid's Google Account

Chrome for Android offers features to be used when signed in with a [kid's Google Account](#) and automatically signs in a

kid's account if they've signed into the Android device. Chrome uses the Sync feature to sync settings configured by parents to the kid's account. You can read about how Sync data is used in the [Sign in](#) section of this Whitepaper.

The collection and use of Chrome data in association with a kid's Google Account are governed by the [Google Family Link - Children's Privacy Policy](#).

In order for the configured settings to apply to a kid's account, Chrome does not support the following features for a kid's Google Account: signing out of Chrome, [Incognito mode](#), and deleting browsing history from within Chrome. Browsing history can still be removed in the [Chrome section of the Google Dashboard](#).

By default, first party cookie blocking is disabled when Chrome is signed in with a kid's account. Parents can go to chrome.google.com/manage/family to allow their kids to block first party cookies. However, blocking cookies signs kids out of Google web products such as Google Search or YouTube and therefore prevents these products from providing any features designed for kids' Google Accounts.

When Chrome is used with a kid's Google Account, information about the kid's requests to access blocked content is sent to Google and made visible to the kid's parent(s) on chrome.google.com/manage/family and in the [Google Family Link app](#). If the kid's browsing mode is set to "Try to block mature sites", Chrome will send a request to the Google [SafeSearch service](#) for each navigation in order to block access to sites that have been classified as containing mature content.

Incognito and Guest Mode

Incognito mode in Chrome is a temporary browsing mode. It ensures that you don't leave browsing history and cookies on your computer. The browsing history and cookies are deleted only once you have closed the last incognito window. Incognito mode cannot make you invisible on the internet. Websites that you navigate to may record your visits. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Browsing as a Guest in Chrome allows you to use somebody else's computer without modifying their profile. For example, no bookmarks or passwords get stored on their computer. Note that Guest mode does not protect you for example, if the computer you are using is infected by a keylogger that records what you type.

iOS 8 and Mac OS X Yosemite Handoff Support

While browsing in a standard (i.e. non-Incognito) session, Chrome will share your current URL with iOS 8+ to support the Handoff feature that was added in OS X Yosemite. This information is only sent to Apple devices that are paired with your iOS device, and the data is encrypted in transit.

More information is available at [Apple Support](#), [Apple Developers](#), and in the [Apple iOS Security Guide](#). Chrome support for this feature can be disabled in Chrome settings.

Security Key

A FIDO U2F Security Key provides a non-phishable credential which can be used to authenticate a user. This mitigates the risk of various kinds of man-in-the-middle attacks in which websites try to steal your password and use it later.

To prevent abuse, a website is required to be delivered over a secure connection (HTTPS), and to register the security key before it can be used for identification. Once a website is registered with a specific security key, that security key will provide a persistent identifier, regardless of which computer it is plugged into, or whether you're in incognito or guest mode, but you must physically interact with the security key to give a website access to an identifier (by, for example, touching it, or plugging it in).

Physical Web

The Physical Web lets you see a list of URLs being broadcast by objects in the environment around you. Google Chrome looks for Physical Web devices with Bluetooth Low Energy beacons that are broadcasting URLs using the Eddystone protocol. Bluetooth signals can be received from 90 feet away or more, depending on signal strength and the user's environment (although the range is often much shorter, due to obstacles and signal noise). If the Physical Web feature is enabled, Chrome sends detected URLs to Google's Physical Web Service (PWS) via a cookieless HTTPS request. For each URL, the PWS obtains the title of the web page, filters out unsafe results, and returns a ranking based on non-personalized signals about the quality and relevance of the web page.

The Physical Web feature is available on Chrome on iOS and Android. Users will need to turn on Bluetooth to use the feature.

If Android users have location settings enabled on both their device and in Chrome, they will receive a notification the first time they are near a beacon that will give them the option to turn on the Physical Web feature. This beacon's URL is not sent to Google's PWS unless the Physical Web feature is enabled. Users can also [enable](#) (or disable) the feature in the Privacy settings. Once a user enables the feature, Chrome scans for nearby devices for a few seconds each time the user unlocks the mobile device in use and sends them to the PWS in order to obtain more information about the beacon. The user receives a silent notification when Chrome finds a nearby URL.

On iOS devices, users can [enable](#) (or disable) the feature in the Privacy settings or by adding the [Chrome widget to their Today view](#) in the notification center. Additionally, the feature is automatically enabled for users who have location enabled on their device, granted Chrome the location permission, and have granted Google the geolocation

permission. Chrome scans for nearby devices whenever it is open in the foreground. When Chrome finds nearby URLs, users will see them as omnibox suggestions. Additionally, Chrome scans for nearby devices for a few seconds when the Today widget is displayed in the notification center.

Bluetooth

Google Chrome supports the [Web Bluetooth API](#), which provides websites with access to nearby [Bluetooth Low Energy devices](#) with your consent.

Chrome does not let any page communicate with a device unless you explicitly consent. When a web page asks to pair with a device, Chrome will ask you to choose which device the web page should access, if any. Selecting a device for one page does not give other pages access to the device you have chosen, and does not allow that page to access other devices. Currently, permission for a page to communicate with a device is usually revoked when the page is reloaded, and is always revoked when Chrome is restarted.

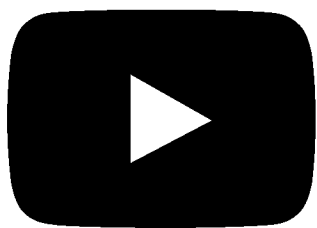
Chrome data that Android sends to Google

The data collection and usage described in this section is handled by Android and governed by the [Google Privacy Policy](#).

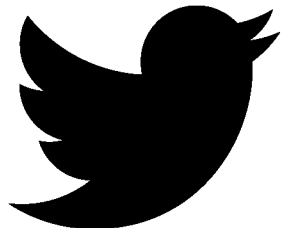
If the Android Backup Service is enabled on your device, some of your Chrome preferences will be saved and stored on Google servers. For Nexus and Android One devices, it is described under “Back up your data and settings with Android Backup Service” in [this article](#). For other Android devices, you may be able to find help by looking up your device on [this page](#). When setting up a new Android device, you may request that it copies the preferences from a previously set up device. If you do so, Android may restore backed up Chrome preferences when Chrome is first installed. The new device only copies the preferences if automatic restore is enabled (see “Restore your data and settings” in [the same article](#)), Chrome was signed into an account when the backup was made, and the new Android device is signed into that same account.

Chrome’s backup data for a particular device may also be restored if you uninstall and then later re-install Chrome on that device. This will only happen if automatic restore is enabled and the device is signed into the account that Chrome was signed into when the backup was made.

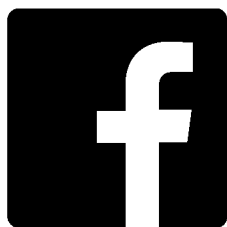
Follow us



.



.



.



Chrome Family

- [Other Platforms](#)
- [Chromebooks](#)
- [Chromecast](#)
- [Chrome Cleanup Tool](#)



Enterprise

- [Google Chrome Browser](#)
- [Devices](#)
- [Google Cloud](#)
- [G Suite](#)



Education

- [Google Chrome Browser](#)
- [Devices](#)
- [Web Store](#)



Dev and Partners

- [Chromium](#)
- [Chrome OS](#)
- [Chrome Web Store](#)
- [Chrome Experiments](#)
- [Chrome Beta](#)
- [Chrome Dev](#)
- [Chrome Canary](#)



Stay Connected

- [Google Chrome Blog](#)
- [Chrome Help](#)

Google

- [Privacy and Terms](#)
- [About Google](#)
- [Google Products](#)



[Help](#)

[Close](#)

Download Chrome for Windows

For Windows 10/8.1/8/7 32-bit.

For Windows 10/8.1/8/7 64-bit.

This computer will no longer receive Google Chrome updates because Windows XP and Windows Vista are no longer supported.

Download Chrome for Mac

For Mac OS X 10.10 or later.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

Download Chrome for Linux

Debian/Ubuntu/Fedora/openSUSE.

Please select your download package:

- ☒ 64 bit .deb (For Debian/Ubuntu)
- ☐ 64 bit .rpm (For Fedora/openSUSE)

Not Debian/Ubuntu or Fedora/openSUSE? There may be a community-supported version for your distribution [here](#).

Download Chrome for iOS

Google Chrome Terms of Service

These Terms of Service apply to the executable code version of Google Chrome. Source code for Google Chrome is available free of charge under open source software license agreements at <https://code.google.com/chromium/terms.html>.

1. Your relationship with Google

1.1 Your use of Google's products, software, services and web sites (referred to collectively as the "Services" in this document and excluding any services provided to you by Google under a separate written agreement) is subject to the terms of a legal agreement between you and Google. "Google" means Google Inc., whose principal place of business is at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States. This document explains how the agreement is made up, and sets out some of the terms of that agreement.

1.2 Unless otherwise agreed in writing with Google, your agreement with Google will always include, at a minimum, the terms and conditions set out in this document. These are referred to below as the "Universal Terms". Open source software licenses for Google Chrome source code constitute separate written agreements. To the limited extent that the open source software licenses expressly supersede these Universal Terms, the open source licenses govern your agreement with Google for the use of Google Chrome or specific included components of Google Chrome.

1.3 Your agreement with Google will also include the terms set forth below in the Google Chrome Additional Terms of Service and terms of any Legal Notices applicable to the Services, in addition to the Universal Terms. All of these are referred to below as the "Additional Terms". Where Additional Terms apply to a Service, these will be accessible for you to read either within, or through your use of, that Service.

1.4 The Universal Terms, together with the Additional Terms, form a legally binding agreement between you and Google in relation to your use of the Services. It is important that you take the time to read them carefully. Collectively, this legal agreement is referred to below as the "Terms".

1.5 If there is any contradiction between what the Additional Terms say and what the Universal Terms say, then the Additional Terms shall take precedence in relation to that Service.

2.1 In order to use the Services, you must first agree to the Terms. You may not use the Services if you do not accept the Terms.

2.2 You can accept the Terms by:

(A) clicking to accept or agree to the Terms, where this option is made available to you by Google in the user interface for any Service; or

(B) by actually using the Services. In this case, you understand and agree that Google will treat your use of the Services as acceptance of the Terms from that point onwards.

3. Language of the Terms

3.1 Where Google has provided you with a translation of the English language version of the Terms, then you agree that the translation is provided for your convenience only and that the English language versions of the Terms will govern your relationship with Google.

3.2 If there is any contradiction between what the English language version of the Terms says and what a translation says, then the English language version shall take precedence.

4. Provision of the Services by Google

4.1 Google has subsidiaries and affiliated legal entities around the world ("Subsidiaries and Affiliates"). Sometimes, these companies will be providing the Services to you on behalf of Google itself. You acknowledge and agree that Subsidiaries and Affiliates will be entitled to provide the Services to you.

4.2 Google is constantly innovating in order to provide the best possible experience for its users. You acknowledge and agree that the form and nature of the Services which Google provides may change from time to time without prior notice to you.

4.3 As part of this continuing innovation, you acknowledge and agree that Google may stop (permanently or temporarily) providing the Services (or any features within the Services) to you or to users generally at Google's sole discretion, without prior notice to you. You may stop using the Services at any time. You do not need to specifically inform Google when you stop using the Services.

4.4 You acknowledge and agree that if Google disables access to your account, you may be prevented from accessing the Services, your account details or any files or other content which is contained in your account.

5. Use of the Services by you

5.1 You agree to use the Services only for purposes that are permitted by (a) the Terms and (b) any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries).

5.2 You agree that you will not engage in any activity that interferes with or disrupts the Services (or the servers and networks which are connected to the Services).

5.3 Unless you have been specifically permitted to do so in a separate agreement with Google, you agree that you will not reproduce, duplicate, copy, sell, trade or resell the Services for any purpose.

5.4 You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) any breach of your obligations under the Terms and for the consequences (including any loss or damage which Google may suffer) of any such breach.

6. Privacy and your personal information

6.1 For information about Google's data protection practices, please read Google's privacy policy at <https://www.google.com/privacy.html> and at <https://www.google.com/intl/en/chrome/privacy/>. This policy explains how Google treats your personal information, and protects your privacy, when you use the Services.

6.2 You agree to the use of your data in accordance with Google's privacy policies.

7. Content in the Services

7.1 You understand that all information (such as data files, written text, computer software, music, audio files or other sounds, photographs, videos or other images) which you may have access to as part of, or through your use of, the Services are the sole responsibility of the person from which such content originated. All such information is referred to below as the "Content."

7.2 You should be aware that Content presented to you as part of the Services, including but not limited to advertisements in the Services and sponsored Content within the Services may be protected by intellectual property rights which are owned by the sponsors or advertisers who provide that Content to Google (or by other persons or companies on their behalf). You may not modify, rent, lease, loan, sell, distribute or create derivative works based on this Content (either in whole or in part) unless you have been specifically told that you may do so by Google or by the owners of that Content, in a separate agreement.

7.3 Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some of the Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings (see <https://support.google.com/websearch/answer/510?hl=en>). In addition, there are commercially available services and software to limit access to material that you may find objectionable.

7.4 You understand that by using the Services you may be exposed to Content that you may find offensive, indecent or objectionable and that, in this respect, you use the Services at your own risk.

7.5 You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) any Content that you create, transmit or display while using the Services and for the consequences of your actions (including any loss or damage which Google may suffer) by doing so.

8. Proprietary rights

8.1 You acknowledge and agree that Google (or Google's licensors) own all legal right, title and interest in and to the Services, including any intellectual property rights which subsist in the Services (whether those rights happen to be registered or not, and wherever in the world those rights may exist).

8.2 Unless you have agreed otherwise in writing with Google, nothing in the Terms gives you a right to use any of Google's trade names, trade marks, service marks, logos, domain names, and other distinctive brand features.

8.3 If you have been given an explicit right to use any of these brand features in a separate written agreement with Google, then you agree that your use of such features shall be in compliance with that agreement, any applicable provisions of the Terms, and Google's brand feature use guidelines as updated from time to time. These guidelines can be viewed online at <https://www.google.com/permissions/guidelines.html> (or such other URL as Google may provide for this purpose from time to time).

8.4 Google acknowledges and agrees that it obtains no right, title or interest from you (or your licensors) under these Terms in or to any Content that you submit, post, transmit or display on, or through, the Services, including any intellectual property rights which subsist in that Content (whether those rights happen to be registered or not, and wherever in the world those rights may exist). Unless you have agreed otherwise in writing with Google, you agree that you are responsible for protecting and enforcing those rights and that Google has no obligation to do so on your behalf.

8.5 You agree that you shall not remove, obscure, or alter any proprietary rights notices (including copyright and trade mark notices) which may be affixed to or contained within the Services.

8.6 Unless you have been expressly authorized to do so in writing by Google, you agree that in using the Services, you will not use any trade mark, service mark, trade name, logo of any company or organization in a way that is likely or intended to cause confusion about the owner or authorized user of such marks, names or logos.

9. License from Google

9.1 Google gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by Google as part of the Services as provided to you by Google (referred to as the "Software" below). This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Google, in the manner permitted by the Terms.

9.2 Subject to section 1.2, you may not (and you may not permit anyone else to) copy, modify, create a derivative work of, reverse engineer, decompile or otherwise attempt to extract the source code of the Software or any part thereof, unless this is expressly permitted or required by law, or unless you have been specifically told that you may do so by Google, in writing.

9.3 Subject to section 1.2, unless Google has given you specific written permission to do so, you may not assign (or grant a sub-license of) your rights to use the Software, grant a security interest in or over your rights to use the Software, or otherwise transfer any part of your rights to use the Software.

10. Content license from you

10.1 You retain copyright and any other rights you already hold in Content which you submit, post or display on or through, the Services.

11. Software updates

11.1 The Software which you use may automatically download and install updates from time to time from Google. These updates are designed to improve, enhance and further develop the Services and may take the form of bug fixes, enhanced functions, new software modules and completely new versions. You agree to receive such updates (and permit Google to deliver these to you) as part of your use of the Services.

12. Ending your relationship with Google

12.1 The Terms will continue to apply until terminated by either you or Google as set out below.

12.2 Google may at any time, terminate its legal agreement with you if:

(A) you have breached any provision of the Terms (or have acted in manner which clearly shows that you do not intend to, or are unable to comply with the provisions of the Terms); or

(B) Google is required to do so by law (for example, where the provision of the Services to you is, or becomes, unlawful); or

(C) the partner with whom Google offered the Services to you has terminated its relationship with Google or ceased to offer the Services to you; or

(D) Google is transitioning to no longer providing the Services to users in the country in which you are resident or from which you use the service; or

(E) the provision of the Services to you by Google is, in Google's opinion, no longer commercially viable.

12.3 Nothing in this Section shall affect Google's rights regarding provision of Services under Section 4 of the Terms.

12.4 When these Terms come to an end, all of the legal rights, obligations and liabilities that you and Google have benefited from, been subject to (or which have accrued over time whilst the Terms have been in force) or which are expressed to continue indefinitely, shall be unaffected by this cessation, and the provisions of paragraph 19.7 shall continue to apply to such rights, obligations and liabilities indefinitely.

13. EXCLUSION OF WARRANTIES

13.1 NOTHING IN THESE TERMS, INCLUDING SECTIONS 13 AND 14, SHALL EXCLUDE OR LIMIT GOOGLE'S WARRANTY OR LIABILITY FOR LOSSES WHICH MAY NOT BE LAWFULLY EXCLUDED OR LIMITED BY APPLICABLE LAW. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR CONDITIONS OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR LOSS OR DAMAGE CAUSED BY NEGLIGENCE, BREACH OF CONTRACT OR BREACH OF IMPLIED TERMS, OR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, ONLY THE LIMITATIONS WHICH ARE LAWFUL IN YOUR JURISDICTION WILL APPLY TO YOU AND OUR LIABILITY WILL BE LIMITED TO THE MAXIMUM EXTENT PERMITTED BY LAW.

13.2 YOU EXPRESSLY UNDERSTAND AND AGREE THAT YOUR USE OF THE SERVICES IS AT YOUR SOLE RISK AND THAT THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE."

13.3 IN PARTICULAR, GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO YOU THAT:

(A) YOUR USE OF THE SERVICES WILL MEET YOUR REQUIREMENTS,

(B) YOUR USE OF THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR,

(C) ANY INFORMATION OBTAINED BY YOU AS A RESULT OF YOUR USE OF THE SERVICES WILL BE ACCURATE OR RELIABLE, AND

(D) THAT DEFECTS IN THE OPERATION OR FUNCTIONALITY OF ANY SOFTWARE PROVIDED TO YOU AS PART OF THE SERVICES WILL BE CORRECTED.

13.4 ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICES IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR OTHER DEVICE OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL.

13.5 NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM GOOGLE OR THROUGH OR FROM THE SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TERMS.

13.6 GOOGLE FURTHER EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

14. LIMITATION OF LIABILITY

14.1 SUBJECT TO OVERALL PROVISION IN PARAGRAPH 13.1 ABOVE, YOU EXPRESSLY UNDERSTAND AND AGREE THAT GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS SHALL NOT BE LIABLE TO YOU FOR:

(A) ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL CONSEQUENTIAL OR EXEMPLARY DAMAGES WHICH MAY BE INCURRED BY YOU, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY.. THIS SHALL INCLUDE, BUT NOT BE LIMITED TO, ANY LOSS OF PROFIT (WHETHER INCURRED DIRECTLY OR INDIRECTLY), ANY LOSS OF GOODWILL OR BUSINESS REPUTATION, ANY LOSS OF DATA SUFFERED, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR OTHER INTANGIBLE LOSS;

(B) ANY LOSS OR DAMAGE WHICH MAY BE INCURRED BY YOU, INCLUDING BUT NOT LIMITED TO LOSS OR DAMAGE AS A RESULT OF:

(I) ANY RELIANCE PLACED BY YOU ON THE COMPLETENESS, ACCURACY OR EXISTENCE OF ANY ADVERTISING, OR AS A RESULT OF ANY RELATIONSHIP OR TRANSACTION BETWEEN YOU AND ANY ADVERTISER OR SPONSOR WHOSE ADVERTISING APPEARS ON THE SERVICES;

(II) ANY CHANGES WHICH GOOGLE MAY MAKE TO THE SERVICES, OR FOR ANY PERMANENT OR TEMPORARY CESSATION IN THE PROVISION OF THE SERVICES (OR ANY FEATURES WITHIN THE SERVICES);

(III) THE DELETION OF, CORRUPTION OF, OR FAILURE TO STORE, ANY CONTENT AND OTHER

(IV) YOUR FAILURE TO PROVIDE GOOGLE WITH ACCURATE ACCOUNT INFORMATION;

(V) YOUR FAILURE TO KEEP YOUR PASSWORD OR ACCOUNT DETAILS SECURE AND CONFIDENTIAL;

14.2 THE LIMITATIONS ON GOOGLE'S LIABILITY TO YOU IN PARAGRAPH 14.1 ABOVE SHALL APPLY WHETHER OR NOT GOOGLE HAS BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING.

15. Copyright and trade mark policies

15.1 It is Google's policy to respond to notices of alleged copyright infringement that comply with applicable international intellectual property law (including, in the United States, the Digital Millennium Copyright Act) and to terminating the accounts of repeat infringers. Details of Google's policy can be found at <https://www.google.com/dmca.html>.

15.2 Google operates a trade mark complaints procedure in respect of Google's advertising business, details of which can be found at https://www.google.com/tm_complaint.html.

16. Advertisements

16.1 Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.

16.2 The manner, mode and extent of advertising by Google on the Services are subject to change without specific notice to you.

16.3 In consideration for Google granting you access to and use of the Services, you agree that Google may place such advertising on the Services.

17. Other content

17.1 The Services may include hyperlinks to other web sites or content or resources. Google may have no control over any web sites or resources which are provided by companies or persons other than Google.

17.2 You acknowledge and agree that Google is not responsible for the availability of any such external sites or resources, and does not endorse any advertising, products or other materials on or available from such web sites or resources.

17.3 You acknowledge and agree that Google is not liable for any loss or damage which may be incurred by you as a result of the availability of those external sites or resources, or as a result of any reliance placed by you on the completeness, accuracy or existence of any advertising, products or other materials on, or available from, such web sites or resources.

18. Changes to the Terms

18.1 Google may make changes to the Universal Terms or Additional Terms from time to time. When these changes are made, Google will make a new copy of the Universal Terms available at https://www.google.com/intl/en/chrome/privacy/eula_text.html and any new Additional Terms will be made available to you from within, or through, the affected Services.

18.2 You understand and agree that if you use the Services after the date on which the Universal Terms or Additional Terms have changed, Google will treat your use as acceptance of the updated Universal Terms or Additional Terms.

19. General legal terms

19.1 Sometimes when you use the Services, you may (as a result of, or in connection with your use of the Services) use a service or download a piece of software, or purchase goods, which are provided by another person or company. Your use of these other services, software or goods may be subject to separate terms between you and the company or person concerned. If so, the Terms do not affect your legal relationship with these other companies or individuals.

19.2 The Terms constitute the whole legal agreement between you and Google and govern your use of the Services (but excluding any services which Google may provide to you under a separate written agreement), and completely replace any prior agreements between you and Google in relation to the Services.

19.3 You agree that Google may provide you with notices, including those regarding changes to the Terms, by email, regular mail, or postings on the Services.

19.4 You agree that if Google does not exercise or enforce any legal right or remedy which is contained in the Terms (or which Google has the benefit of under any applicable law), this will not be taken to be a formal waiver of Google's rights and that those rights or remedies will still be available to Google.

19.5 If any court of law, having the jurisdiction to decide on this matter, rules that any provision of these Terms is invalid, then that provision will be removed from the Terms without affecting the rest of the Terms. The remaining provisions of the Terms will continue to be valid and enforceable.

19.6 You acknowledge and agree that each member of the group of companies of which Google is the parent shall be third party beneficiaries to the Terms and that such other companies shall be entitled to directly enforce, and rely upon, any provision of the Terms which confers a benefit on (or rights in favor of) them. Other than this, no other person or company shall be third party beneficiaries to the Terms.

19.7 The Terms, and your relationship with Google under the Terms, shall be governed by the laws of the State of California without regard to its conflict of laws provisions. You and Google agree to submit to the exclusive jurisdiction of the courts located within the county of Santa Clara, California to resolve any legal matter arising from the Terms. Notwithstanding this, you agree that Google shall still be allowed to apply for injunctive remedies (or an equivalent type of urgent legal relief) in any jurisdiction.

20. Additional Terms for Extensions for Google Chrome

20.1 These terms in this section apply if you install extensions on your copy of Google Chrome. Extensions are small software programs, developed by Google or third parties, that can modify and enhance the functionality of Google Chrome. Extensions may have greater privileges to access your browser or your computer than regular webpages, including the ability to read and modify your private data.

20.2 From time to time, Google Chrome may check with remote servers (hosted by Google or by third parties) for available updates to extensions, including but not limited to bug fixes or enhanced functionality. You agree that such updates will be automatically requested, downloaded, and installed without further notice to you.

20.3 From time to time, Google may discover an extension that violates Google developer terms or other legal agreements, laws, regulations or policies. Google Chrome will periodically download a list of such extensions from Google's servers. You agree that Google may remotely disable or remove any such extension from user systems in its sole discretion.

21. Additional Terms for Enterprise Use

21.1 If you are a business entity, then the individual accepting on behalf of the entity (for the avoidance of doubt, for business entities, in these Terms, "you" means the entity) represents and warrants that he or she has the authority to act on your behalf, that you represent that you are duly authorized to do business in the country or countries where you operate, and that your employees, officers, representatives, and other agents accessing the Service are duly authorized to access Google Chrome and to legally bind you to these Terms.

21.2 Subject to the Terms, and in addition to the license grant in Section 9, Google grants you a non-exclusive, non-transferable license to reproduce, distribute, install, and use Google Chrome solely on machines intended for use by your employees, officers, representatives, and agents in connection with your business entity, and provided that their use of Google Chrome will be subject to the Terms.

August 12, 2010

Google Chrome Additional Terms of Service

MPEG LA

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PARTNER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Adobe

Google Chrome may include one or more components provided by Adobe Systems Incorporated and Adobe Software Ireland Limited (collectively "Adobe"). Your use of the Adobe software as provided by Google ("Adobe Software") is subject to the following additional terms (the "Adobe Terms"). You, the entity receiving the Adobe Software, will be hereinafter referred to as "Sublicensee."

1. License Restrictions.

(a) Flash Player, Version 10.x is designed only as a browser plug-in. Sublicensee may not modify or distribute this Adobe Software for use as anything but a browser plug-in for playing back content on a web page. For example, Sublicensee will not modify this Adobe Software in order to allow interoperation with applications that run outside of the browser (e.g., standalone applications, widgets, device UI).

(b) Sublicensee will not expose any APIs of the Flash Player, Version 10.x through a browser plug-in interface in such a way that allows such extension to be used to playback content from a web page as a stand-alone application.

(c) The Chrome-Reader Software may not be used to render any PDF or EPUB documents that utilize digital rights management protocols or systems other than Adobe DRM.

(d) Adobe DRM must be enabled in the Chrome-Reader Software for all Adobe DRM protected PDF and EPUB documents.

Case 4:20-cv-03664-YGR Document 666-14 Filed 08/05/22 Page 55 of 110

(e) The Chrome Reader Software may not, other than as explicitly permitted by the technical specifications, disable any capabilities provided by Adobe in the Adobe Software, including but not limited to, support for PDF and EPUB formats and Adobe DRM.

2. Electronic Transmission. Sublicensee may allow the download of the Adobe Software from a web site, the Internet, an intranet, or similar technology (an, "Electronic Transmissions") provided that Sublicensee agrees that any distributions of the Adobe Software by Sublicensee, including those on CD-ROM, DVD-ROM or other storage media and Electronic Transmissions, if expressly permitted, shall be subject to reasonable security measures to prevent unauthorized use. With relation to Electronic Transmissions approved hereunder, Sublicensee agrees to employ any reasonable use restrictions set by Adobe, including those related to security and/or the restriction of distribution to end users of the Sublicensee Product.

3. EULA and Distribution Terms.

(a) Sublicensee shall ensure that the Adobe Software is distributed to end users under an enforceable end user license agreement, in favor of Sublicensee and its suppliers containing at least each of the following minimum terms (the "End-User License"): (i) a prohibition against distribution and copying, (ii) a prohibition against modifications and derivative works, (iii) a prohibition against decompiling, reverse engineering, disassembling, and otherwise reducing the Adobe Software to a human-perceivable form, (iv) a provision indicating ownership of Sublicensee Product (as defined in Section 8) by Sublicensee and its licensors, (v) a disclaimer of indirect, special, incidental, punitive, and consequential damages, and (vi) other industry standard disclaimers and limitations, including, as applicable: a disclaimer of all applicable statutory warranties, to the full extent allowed by law.

(b) Sublicensee shall ensure that the Adobe Software is distributed to Sublicensee's distributors under an enforceable distribution license agreement, in favor of Sublicensee and its suppliers containing terms as protective of Adobe as the Adobe Terms.

4. Opensource. Sublicensee will not directly or indirectly grant, or purport to grant, to any third party any rights or immunities under Adobe's intellectual property or proprietary rights that will subject such intellectual property to an open source license or scheme in which there is or could be interpreted to be a requirement that as a condition of use, modification and/or distribution, the Adobe Software be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; or (iii) redistributable at no charge. For clarification purposes, the foregoing restriction does not preclude Sublicensee from distributing, and Sublicensee will distribute the Adobe Software as bundled with the Google Software, without charge.

5. Additional Terms. With respect to any update, upgrade, new versions of the Adobe Software (collectively "Upgrades") provided to Sublicensees, Adobe reserves the right to require additional terms and conditions applicable solely to the Upgrade and future versions thereof, and solely to the extent that such restrictions are imposed by Adobe on all licensees of such Upgrade. If Sublicensee does not agree to such additional terms or conditions, Sublicensee will have no license rights with respect to such Upgrade, and Sublicensee's license rights with respect to the Adobe Software will terminate automatically on the 90th day from the date such additional terms are made available to Sublicensee.

6. Proprietary Rights Notices. Sublicensee shall not, and shall require its distributors not to, delete or in any manner alter the copyright notices, trademarks, logos or related notices, or other proprietary rights notices of Adobe (and its licensors, if any) appearing on or within the Adobe Software or accompanying materials.

7. Technical Requirements. Sublicensee and its distributors may only distribute Adobe Software and/or Upgrade on devices that (i) meet the technical specifications posted on <http://www.adobe.com/mobile/licensees>, (or a successor web site thereto), and (ii) has been verified by Adobe as set forth below.

8. Verification and Update. Sublicensee must submit to Adobe each Sublicensee product (and each version thereof) containing the Adobe Software and/or Upgrade ("Sublicensee Product") that do not meet the Device Verification exemption criteria to be communicated by Google, for Adobe to verify. Sublicensee shall pay for each submission made by Sublicensee by procuring verification packages at Adobe's then-current terms set forth at <http://flashmobile.adobe.com/>. Sublicensee Product that has not passed verification may not be distributed. Verification will be accomplished in accordance with Adobe's then-current process described at <http://flashmobile.adobe.com/> ("Verification").

9. Profiles and Device Central. Sublicensee will be prompted to enter certain profile information about the Sublicensee Products either as part of the Verification process or some other method, and Sublicensee will provide such information, to Adobe. Adobe may (i) use such profile information as reasonably necessary to verify the Sublicensee Product (if such product is subject to Verification), and (ii) display such profile information in "Adobe Device Intelligence system," located at <https://devices.adobe.com/partnerportal/>, and made available through Adobe's authoring and development tools and services to enable developers and end users to see how content or applications are displayed in Sublicensee Products (e.g. how video images appear in certain phones).

10. Export. Sublicensee acknowledges that the laws and regulations of the United States restrict the export and re-export of commodities and technical data of United States origin, which may include the Adobe Software. Sublicensee agrees that it will not export or re-export the Adobe Software, without the appropriate United States and foreign governmental clearances, if any.

11. Technology Pass-through Terms.

(a) Except pursuant to applicable permissions or agreements therefor, from or with the applicable parties, Sublicensees shall not use and shall not allow the use of, the Adobe Software for the encoding or decoding of mp3 audio only (.mp3) data on any non-pc device (e.g., mobile phone or set-top box), nor may the mp3 encoders or decoders contained in the Adobe Software be used or accessed by any product other than the Adobe Software. The Adobe Software may be used

for the encoding or decoding of MP3 data contained within a swf or flv file, which contains video, picture or other data. Sublicensee shall acknowledge that use of the Adobe Software for non-PC devices, as described in the prohibitions in this section, may require the payment of licensing royalties or other amounts to third parties who may hold intellectual property rights related to the MP3 technology and that Adobe nor Sublicensee has not paid any royalties or other amounts on account of third party intellectual property rights for such use. If Sublicensee requires an MP3 encoder or decoder for such use, Sublicensee is responsible for obtaining the necessary intellectual property license, including any applicable patent rights.

(b) Sublicensee will not use, copy, reproduce and modify (i) the On2 source code (provided hereunder as a component of the Source Code) as necessary to enable the Adobe Software to decode video in the Flash video file format (.flv or .f4v), and (ii) the Sorenson Spark source code (provided hereunder as a component of the Source Code) for the limited purpose of making bug fixes and performance enhancements to the Adobe Software. All codecs provided with the Adobe Software may only be used and distributed as an integrated part of the Adobe Software and may not be accessed by any other application, including other Google applications.

(c) The Source Code may be provided with an AAC codec and/or HE-AAC codec ("the AAC Codec"). Use of the AAC Codec is conditioned on Sublicensee obtaining a proper patent license covering necessary patents as provided by VIA Licensing, for end products on or in which the AAC Codec will be used. Sublicensee acknowledges and agrees that Adobe is not providing a patent license for an AAC Codec under this Agreement to Sublicensee or its sublicensees.

(d) THE SOURCE CODE MAY CONTAIN CODE LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR WILL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. See <http://www.mpegla.com>

12. Update. Sublicensee will not circumvent Google's or Adobe's efforts to update the Adobe Software in all Sublicensee's products incorporating the Adobe Software as bundled with the Google Software ("Sublicensee Products").

13. Attribution and Proprietary Notices. Sublicensee will list the Adobe Software in publicly available Sublicensee Product specifications and include appropriate Adobe Software branding (specifically excluding the Adobe corporate logo) on the Sublicensee Product packaging or marketing materials in a manner consistent with branding of other third party products contained within the Sublicensee Product.

14. No Warranty. THE ADOBE SOFTWARE IS MADE AVAILABLE TO SUBLICENSEE FOR USE AND REPRODUCTION "AS IS" AND ADOBE MAKES NO WARRANTY AS TO ITS USE OR PERFORMANCE. ADOBE AND ITS SUPPLIERS DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS OBTAINED BY USING THE ADOBE SOFTWARE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO SUBLICENSEE IN SUBLICENSEE'S JURISDICTION, ADOBE AND ITS SUPPLIERS MAKE NO WARRANTIES, CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING WITHOUT LIMITATION NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, SATISFACTORY QUALITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. SUBLICENSEE AGREES THAT SUBLICENSEE SHALL NOT MAKE ANY WARRANTY, EXPRESS OR IMPLIED, ON BEHALF OF ADOBE.

15. Limitation of Liability. IN NO EVENT WILL ADOBE OR ITS SUPPLIERS BE LIABLE TO SUBLICENSEE FOR ANY DAMAGES, CLAIMS OR COSTS WHATSOEVER OR ANY CONSEQUENTIAL, INDIRECT, OR INCIDENTAL DAMAGES, OR ANY LOST PROFITS OR LOST SAVINGS, EVEN IF AN ADOBE REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS, DAMAGES, CLAIMS OR COSTS OR FOR ANY CLAIM BY ANY THIRD PARTY. THE FOREGOING LIMITATIONS AND EXCLUSIONS APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW IN SUBLICENSEE'S JURISDICTION. ADOBE'S AGGREGATE LIABILITY AND THAT OF ITS SUPPLIERS UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO ONE THOUSAND DOLLARS (US\$1,000). Nothing contained in this Agreement limits Adobe's liability to Sublicensee in the event of death or personal injury resulting from Adobe's negligence or for the tort of deceit (fraud). Adobe is acting on behalf of its suppliers for the purpose of disclaiming, excluding and/or limiting obligations, warranties and liability as provided in this Agreement, but in no other respects and for no other purpose.

16. Content Protection Terms

(a) Definitions.

"Compliance and Robustness Rules" means the document setting forth compliance and robustness rules for the Adobe Software located at <http://www.adobe.com/mobile/licensees>, or a successor web site thereto.

"Content Protection Functions" means those aspects of the Adobe Software that are designed to ensure compliance with the Compliance and Robustness Rules, and to prevent playback, copying, modification, redistribution or other actions with respect to digital content distributed for consumption by users of the Adobe Software when such actions are not authorized by the owners of such digital content or its licensed distributors.

"Content Protection Code" means code within certain designated versions of the Adobe Software that enables certain Content Protection Functions.

"Key" means a cryptographic value contained in the Adobe Software for use in decrypting digital content.

(b) License Restrictions. Sublicensee's right to exercise the licenses with respect to the Adobe Software is subject to the following additional restrictions and obligations. Sublicensee will ensure that Sublicensee's customers comply with these restrictions and obligations to the same extent imposed on Sublicensee with respect to the Adobe Software; any failure by Sublicensee's customers to comply with these additional restrictions and obligations shall be treated as a material breach by Sublicensee.

b.1. Sublicensee and customers may only distribute the Adobe Software that meets the Robustness and Compliance Rules as so confirmed by Sublicensee during the verification process described above in the Adobe Terms.

b.2. Sublicensee shall not (i) circumvent the Content Protection Functions of either the Adobe Software or any related Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software or (ii) develop or distribute products that are designed to circumvent the Content Protection Functions of either the Adobe Software or any Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software.

(c) The Keys are hereby designated as Adobe's Confidential Information, and Sublicensee will, with respect to the Keys, adhere to Adobe's Source Code Handling Procedure (to be provided by Adobe upon request).

(d) Injunctive Relief. Sublicensee agrees that a breach of this Agreement may compromise the Content Protection Functions of the Adobe Software and may cause unique and lasting harm to the interests of Adobe and owners of digital content that rely on such Content Protection Functions, and that monetary damages may be inadequate to compensate fully for such harm. Therefore, Sublicensee further agrees that Adobe may be entitled to seek injunctive relief to prevent or limit the harm caused by any such breach, in addition to monetary damages.


17. Intended Third-party Beneficiary. Adobe Systems Incorporated and Adobe Software Ireland Limited are the intended third-party beneficiaries of Google's agreement with Sublicensee with respect to the Adobe Software, including but not limited to, the Adobe Terms. Sublicensee agrees, notwithstanding anything to the contrary in its agreement with Google, that Google may disclose Sublicensee's identity to Adobe and certify in writing that Sublicensee has entered into a license agreement with Google which includes the Adobe Terms. Sublicensee must have an agreement with each of its licensees, and if such licensees are allowed to redistribute the Adobe Software, such agreement will include the Adobe Terms.

[Printer-friendly version](#)

Note: Installing Google Chrome will **add the Google repository** so your system will automatically keep Google Chrome up to date. If you don't want Google's repository, do "sudo touch /etc/default/google-chrome" before installing the package.

☒ Set Google Chrome as my default browser

☒ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. [Learn more](#)

Accept and Install 

Download Chrome

Download for Windows

For Windows 10/8.1/8/7 32-bit

For Windows 10/8.1/8/7 64-bit

This computer will no longer receive Google Chrome updates because Windows XP and Windows Vista are no longer supported.

Download for Mac

Mac OS X 10.10 or later

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

Download for Linux

Debian/Ubuntu/Fedora/openSUSE

Download for phone or tablet

- [Android](#)
- [iOS](#)

Download for another desktop OS

- [Windows 10/8.1/8/7 64-bit](#)

- Windows 10/8.1/8/7-32-bit
- Mac OS X 10.10 or later
- Linux

Frozen versions

- Windows XP
- Windows Vista
- Mac 10.6 - 10.8
- Mac 10.9

Looks like you're already using Chrome browser. Nice!

The device you have runs on Chrome OS, which already has Chrome browser built-in. No need to manually install or update it — with automatic updates, you'll always get the latest version. [Learn more about automatic updates.](#)

Looking for Chrome for a different operating system?

See the [full list of supported operating systems.](#)

EXHIBIT 23



Go g e

[Chrome](#)

[Skip to content](#)

- [Do More with Chrome](#)
- [Extensions](#)
- [Enterprise](#)

Download Chrome

Go g e

[Chrome](#)

- [Do More with Chrome](#)
- [Extensions](#)
- [Enterprise](#)

Google Chrome Privacy Whitepaper

Last modified: December 5, 2018 (Current as of Chrome 71.0.3578.80)

- [Omnibox](#)
- [Network predictions](#)
- [Search locale](#)
- [New Tab page](#)
- [Tap to Search](#)
- [More like this](#)
- [Safe Browsing protection](#)
- [Unwanted software protection](#)
- [Navigation errors](#)
- [Offline Indicator](#)
- [Google update](#)
- [Network time](#)
- [Counting install](#)
- [Measuring promotions](#)
- [Usage stats](#)
- [Google Surveys](#)
- [Spelling suggestions](#)
- [Translate](#)
- [Signing In](#)
- [Autofill](#)
- [Payments](#)
- [Geolocation](#)
- [Speech to text](#)
- [Google Assistant](#)
- [Cloud Print](#)
- [SSL certificate error reporting](#)
- [Token Binding](#)
- [Installed apps](#)
- [Push Messaging](#)
- [Chrome custom tabs](#)
- [Continue where you left off](#)

- [Chrome variations](#)
- [Do Not Track](#)
- [Plugins](#)
- [Media licenses](#)
- [Cloud policy](#)
- [Data Saver \(Chrome mobile\)](#)
- [Supervised users](#)
- [Kid's Google Account](#)
- [Incognito and Guest mode](#)
- [Handoff support](#)
- [Security key](#)
- [Physical web](#)
- [Bluetooth](#)
- [Data sent by Android](#)

This document describes the features in Chrome that communicate with Google, as well as with third-party services (for example, if you've changed your default search engine). This document also describes the controls available to you regarding how your data is used by Chrome. Here we're focusing on the desktop version of Chrome; we touch only tangentially on Chrome OS and Chrome for Mobile. This document does not cover features that are still under development, such as features in the beta, dev and canary channel and active field trials, or Android apps on Chrome OS if Play Apps are enabled.

If you have questions about Google Chrome and Privacy that this document doesn't answer, please contact the privacy team at privacy@chromium.org. We'd be happy to hear from you.

Redesigned Sync and Google service settings

In version 69, we will begin rolling out a new structure for Chrome settings for a small population of users. All settings that control how Google collects data from Chrome have been moved to a new settings page titled "Sync and Google services," combining previous settings from the "Sync" and "Privacy" section of advanced settings.

Additionally, two new data collection settings have been added to this settings page to control when URL-keyed data is collected by Google: "Activity and interactions" and "Make searches and browsing better (Sends URLs of pages you visit to Google)."

"Activity and interactions" controls the collection of URL-keyed data tied to the user's Google Account (for signed in users) for personalization. For example, the URL of the page you are viewing is sent to Google in order to provide better, contextually relevant suggestions in the Omnibox if "Activity and interactions" is turned on and Google is your default search engine. Previously, this URL was sent if history sync was turned on without a custom passphrase.

"Make searches and browsing better" controls the collection of anonymous URL-keyed data that is used to improve Chrome and the user's general browsing experience. For example, Chrome usage statistics include information about the web pages you visit and your usage of them if "Make searches and browsing better" is turned on. Previously, this data was included if history sync was turned on without a custom passphrase.

Both of these settings allow the user to turn off collection of URL-keyed data without turning off the history sync feature.

Finally, users in this population will also see a modified Chrome sync opt-in dialogue. This new version includes language to cover all Google services on the newly revised "Sync and Google services" settings page, including the two new settings controlling collection of URL-keyed data. When the user accepts the new opt-in dialogue, all of these settings are turned on. The user can click "Settings" from the opt-in dialogue to configure exactly which settings they want turned on.

Omnibox

Google Chrome uses a combined [web address and search bar](#) (we call it the "omnibox") at the top of the browser window.

As you use the omnibox, your [default search engine](#) can suggest addresses and search queries that may be of interest to you. These suggestions make navigation and searching faster and easier, and are turned on by default. They can be turned off by unchecking "Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box" in the "Privacy" section of Chrome's settings. They are also disabled in incognito mode.



In order to provide these suggestions, Chrome sends the text you've typed into the omnibox, along with a general categorization (e.g., "URL", "search query", or "unknown"), to your default search engine. Chrome will also send a signal to your default search provider when you focus in the omnibox, telling it to get ready to provide suggestions. Your IP address and certain cookies are also sent to your default search engine with all requests, in order to return the results that are most relevant to you.

If Chrome determines that your typing may contain sensitive information, such as authentication credentials, local file names, or URL data that is normally encrypted, it will not send the typed text.

If Google is your default search engine, when you select one of the omnibox suggestions, Chrome sends your original

search query, the suggestion you selected, and the position of the suggestion back to Google. This information helps improve the quality of the suggestion feature, and it's logged and anonymized in the same manner as Google web searches. Logs of these suggestion requests are retained for two weeks, after which 2% of the log data is randomly selected, anonymized, and retained in order to improve the suggestion feature.

If you've chosen to sync your Chrome history, and if Google is your default search engine, the URL of the page you're viewing is sent to Google in order to provide better, contextually relevant suggestions. URLs are sent only for HTTP pages and HTTPS pages, not other schemes such as file: and ftp:. Additionally, Chrome may present suggestions as soon as you place the cursor in the omnibox, before you start typing. Chrome is in the process of transitioning to a new service to provide these on-focus suggestions. For most users on desktop versions of Chrome, the request and complete set of suggestions are retained on Google servers in order to further improve and personalize the feature. When the URL that triggered the set of suggestions is deleted from your history, the set of suggestions will stop influencing suggestions personalized to you, and will be deleted; otherwise they are retained in your Google account for a year. For a small portion of users on desktop versions of Chrome, and users on mobile versions of Chrome, the logging described in the previous paragraphs apply except that URLs are never included in the 2% sampling of log data.

On Android, your location will also be sent to Google via an X-Geo HTTP request header if Google is your default search engine, the Chrome app has the permission to use your geolocation and you haven't blocked geolocation for www.google.com (or country-specific origins such as www.google.de). Additionally, if your device has network location enabled (High Accuracy or Battery Saving Device Location mode in Android settings), the X-Geo header may also include visible network IDs (WiFi and Cell), used to geocode the request server-side. The X-Geo header will never be sent in Incognito mode. HTTPS will be required to include this header in the request. You can learn more about how to control the Android OS location sharing with apps on [this article](#) for Nexus, or find your device [here](#) if you do not use a Nexus. How to control location sharing with a site within Chrome is written in [this article](#). See the [Geolocation](#) section of this whitepaper for more information on default geolocation permissions.

Additionally, if Google is your search engine and you have enabled sync, omnibox may also show suggestions for your Google Drive files. You can turn this functionality off by disabling the "Drive suggestions" option in Sync settings.

If you use a non-Google search provider as your default search engine, queries are sent and logged under that provider's privacy policy.

Additionally, when you use the omnibox to search for a single word, Chrome may send this word to your DNS server to see whether it corresponds to a host on your network, and may try to connect to the corresponding host. This gives you the option to navigate to that host instead of searching. For example, if your router goes by the hostname "router", and you type "router" in the omnibox, you're given the option to navigate to <https://router/>, as well as to search for the word "router" with your default search provider. This feature is not controlled by the "Use a prediction service to help complete searches and URLs..." option because it does not involve sending data to your default search engine.

Network predictions

Chrome uses a prediction service to load pages more quickly. The prediction service uses navigation history and local heuristics to predict which resources and pages are likely to be needed next, and it initiates actions such as DNS prefetching, TCP and TLS preconnection, and prefetching of web pages. To [turn off](#) network predictions, uncheck "Use a prediction service to load pages more quickly" in the "Privacy" section of Chrome's settings.

To improve load times, the browser can be asked to prefetch links that you might click next. Chrome supports four types of prefetching:

- Chrome prefetching - can be initiated by Chrome itself whenever it detects a search query typed in the omnibox or a likely beginning of a URL you type often
- Webpage prefetching - requested by one web page to prefetch another
- AMP prefetching - can be requested only by the Google Search App on Android to prefetch several accelerated mobile pages (AMP) articles and display them later in a Chrome Custom Tab
- CustomTabs prefetching - any Android app can request to prefetch several URLs to speed up displaying them later in a Chrome Custom Tab

Controlling the feature. All prefetching types except webpage prefetching are controlled by Chrome's prediction service setting. Webpage prefetching is allowed regardless of whether Chrome's network prediction service feature is enabled.

Handling of cookies. The prefetched site is allowed to set and read its own cookies just as if you had visited it (even if you don't end up visiting the prefetched page). All types of prefetching are disabled if you disallow third party cookies to prevent cookies from being set from pages that you did not visit.

Javascript execution. For AMP prefetching the page is fully rendered and Javascript is also executed. For the remaining types of prefetching Javascript is not executed.

Google search locale

If Google is set as your default search engine, Chrome will try to determine the most appropriate locale for Google search queries conducted from the [omnibox](#) in order to give you relevant search results based on your location. For example, if you were in Germany, your omnibox searches may go through google.de instead of google.com.

In order to do this, Chrome will send a request to google.com each time you start the browser. If you already have any cookies from the google.com domain, this request will also include these cookies, and is logged as any normal HTTPS

New Tab page

The Chrome New Tab page may display suggestions for websites that you might want to visit.

In order to help you get started, Chrome may suggest content that is popular in your country or region. Chrome uses your IP address to identify your country or region.

Chrome tries to make personalized suggestions that are useful to you. For this, Chrome uses the sites you have visited from your local browsing history. On Android, the most popular languages of the sites you visited may also be sent to Google to provide suggestions in languages you prefer to read, and the device display DPI may be sent to format content for your device. To save data, Chrome may additionally send a hash of the content that Google provided to you the last time, so that you only download content when there is something new.

If you are signed into Chrome, suggestions are *also* based on data stored in your Google account activity. You can control the collection of data in your Google account at [Activity controls](#) and manage your account activity at [My Activity](#). For example, if you sync your browsing history and have enabled its use in your Web & App activity, Google may suggest sites that relate to sites you have visited in the past. Chrome measures the quality of suggestions by sending Google information about the sets of suggestions that were displayed, and those that were selected.

On the desktop version of Chrome, you may also manually add shortcuts to websites that you regularly visit, or edit Chrome's existing website suggestions. After you add, edit, or delete a shortcut to a website, the Chrome New Tab page will not suggest any new websites to you.

Suggestions generated from your browsing history will be removed once you clear your browsing history. However, if you customized your suggestions, they will not be removed.

For Chrome on Android, in certain countries, Chrome may download the content of the New Tab page suggestions from Google, for use while offline. Chrome sends to Google a cookieless request with the URL for each suggestion, along with Chrome's user agent string, in order to render the content. You can remove downloaded content by clearing Chrome's cache data, or by opening the Downloads menu and [selecting individual pages to delete](#). You can disable this feature by disabling "Automatically download pages" in Chrome's Privacy settings.

For desktop and Android versions of Chrome, when you open a new tab, Chrome loads a New Tab page customized by your default search engine (e.g., google.com) if it's available. This page is preloaded in the background and refreshed periodically so that it opens quickly. Your IP address and cookies, as well as your current browser theme, are sent to your search engine with each refresh request so that the New Tab page can be correctly displayed. See the [Embedded Search API](#) for more details. Your search engine may also record your interactions with the New Tab page.

The New Tab page content may be designed by your default search provider. Suggested websites are embedded by Chrome into the New Tab page in a way that does not expose them to your default search provider.

This information about the New Tab page may not apply if you've installed an extension that [overrides the New Tab page](#).

Tap to Search

If you've enabled "Tap to Search" on Chrome Mobile you can search for terms by tapping them.

When you tap a word, the word, the surrounding text, and the home country of your device's SIM card are sent to Google to identify recommended search terms (for example, tapping on "Michael" on a site about Michael Jackson might lead to a suggested search for "Michael Jackson"). The tapped word is logged in accordance with standard Google logging policies, and the surrounding text and home country are logged only when the page is already in Google's search index. If you sync your browsing history, the URL of the page is also sent and logged, and is used to improve your query suggestions.

When Google returns a search suggestion, a card "peeks through" at the bottom of the screen, showing the suggested search term. Opening this card is considered a regular search and navigation on Google, so standard logging policies apply.

Long-pressing on a word opens a peeking card with the selected word, except on recent versions of [Android Oreo](#) and higher which activates Smart Text Selection instead. No communication with Google occurs until the card is opened, and no surrounding text is sent. Saying "Ok Google" after long-pressing on a word provides the word and its surrounding text as context for the Google Assistant.

Tap to Search is enabled in a limited mode by default: potentially privacy-sensitive data, such as the URL and surrounding text, is not sent for HTTPS pages. Tap to Search can be fully enabled and disabled in the card or in the Chrome privacy settings.

More like this

If you have chosen to sync your browsing history, Chrome may provide contextually relevant content recommendations on certain pages via a "More like this" button on the top toolbar and the suggestions will be shown from a bottom sheet.

In order to provide these suggestions, the URL of the page that you're currently viewing, along with your language or locale information and IP address is sent to Google. Suggestions are only fetched for HTTP and HTTPS pages, not pages with other schemas like file: or ftp:. Selected suggestions are logged in accordance with standard Google logging policies.

Suggestions are not available on all webpages. When there are suggestions, the "More like this" button will appear on the top toolbar.

Safe Browsing protection

Google Chrome includes an optional feature called "Safe Browsing" to help protect you against phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. You can find more information at safebrowsing.google.com about how Safe Browsing protects you in Chrome and other Google products. Safe Browsing is designed specifically to protect your privacy and is also used by other popular browsers. This feature is not available on the iOS version of Chrome.

When Safe Browsing is enabled in Chrome, Chrome contacts Google's servers periodically to download the most recent Safe Browsing list of unsafe extensions and sites, including phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. The most recent copy of this list is stored locally on your system. Chrome checks the URL of each site you visit or file you download against this local list. If you navigate to a URL that appears on the list, Chrome sends a partial URL fingerprint (the first 32 bits of a SHA-256 hash of the URL) to Google for verification that the URL is indeed dangerous. Chrome also sends a partial URL fingerprint when a site requests a potentially dangerous permission, so that Google can protect you if the site is malicious. Google cannot determine the actual URL from this information.

In addition to the URL check described above, Chrome also conducts client-side checks. If a website looks suspicious, Chrome sends a subset of likely phishing and social engineering terms found on the page to Google, in order to determine whether the website should be considered malicious. Chrome can also help protect you from phishing if you type one of your previously saved passwords into an uncommon site. In this case Chrome sends the URL and referrers of the page to Google to see if the page might be trying to steal your password.

If you encounter a website that is on Chrome's Safe Browsing list, you may see a warning like the one shown below. From there, you can choose to opt in to reporting data relevant to security to help improve Safe Browsing and security on the Internet. If you opt in, an incident report will be sent every time you receive a warning or visit a suspicious page. Chrome is currently transitioning this opt-in to change the reporting functionality. If your checkbox reads "Automatically send some system information and page content to Google to help detect dangerous apps and sites" then you are part of the new group of users. This setting differs from the old "report security incidents to Google" in that security reports will also be sent on a very small sample of other sites to help Safe Browsing learn about new threats you may be encountering. This new setting will be unchecked by default even if you opted in to the older setting. The reports are sent to Google over an encrypted channel and can include URLs, headers, and snippets of content from the page and they never include data from browsing you do in Incognito mode. In cases where Chrome discovers unwanted or malicious software on your machine, the reports may also include details about malicious files and registry entries. This data is used only to improve Safe Browsing and to improve security on the Internet. For example, Chrome reports some SSL certificate chains to Google to help improve the accuracy of Chrome's SSL warnings.



You can visit our [malware warning test page](#) or [social engineering warning test page](#) to see the above example in action. For more information about the warning pages, see [Manage warnings about unsafe sites](#). You can find settings for Safe Browsing and the additional reports in the Privacy section of Chrome settings. Please be aware that if you disable the Safe Browsing feature, Chrome will no longer be able to protect you from websites that try to steal your information or install harmful software. We don't recommend turning it off.

If you are a webmaster, developer, or network admin, you can find more relevant information about Safe Browsing on [this page](#).

Safe Browsing also protects you from abusive extensions and malicious software. At start up of Chrome, Safe Browsing scans extensions installed in your browser against the Safe Browsing list. If an extension on the list is found, Chrome will temporarily disable the extension, offer you relevant information and provide an option for you to remove the extension or re-enable it. Chrome also sends the particular extension ID to Safe Browsing. If you attempt to download a file on Chrome's Safe Browsing list, you'll see a warning like this one:



To warn you about potentially dangerous files, like the picture shown above, Chrome checks the URL of potentially dangerous file types you download against a list of URLs that have been verified. This list is stored locally on your computer and updated regularly. Chrome does not send information to Google for files you download from URLs in this list, or if the file is signed by a verified publisher. For all other unverified potentially dangerous file downloads, Chrome sends Google the information needed to help determine whether the download is harmful, including some or all of the following: information about the full URL of the site or file download, all related referrers and redirects, code signing certificates, file hashes, and file header information. Chrome may then show a warning like the one pictured above.

Chrome helps protect you against password phishing by checking with Google when you enter your password on an uncommon page. Chrome keeps a local list of popular websites that Safe Browsing found to be safe. If Chrome detects that you have entered your Google account password or one of your passwords stored in Chrome's password manager

If the reused password is your Google account password and the verdict for the website is that it is phishing, Chrome will suggest that you change your Google account password to avoid losing access to your account. Additionally, if you sync your browsing history without a sync passphrase, Chrome sends another request to tell Google that your password was likely phished, to make hijacking of your Google account by an adversary more difficult. The information sent in this request includes the ID of the synced browsing history entry to identify the URL where the phishing attempt happened, and the verdict received from Safe Browsing.

If you've opted into sharing data relevant to security to help detect dangerous apps and sites, Chrome also sends a request to Safe Browsing each time you start to enter a password on a page that isn't in Chrome's local list. In addition, the request that Chrome sends to Safe Browsing to determine the reputation of the website on which you reuse your password includes the list of websites for which you saved this password in Chrome's password manager (but not the password itself).

If Chrome suspects that your settings have been tampered with, Chrome reports the URL of the last downloaded potentially dangerous file, and information about the nature of the possible tampering, to the Safe Browsing service.

For some downloads, Chrome may ask you to opt in to reporting to Google Safe Browsing some data relevant to security, in order to improve the quality of download protection. Once you've opted in, some downloaded files that are suspicious will be sent to Google for investigation each time they are encountered. You can change this opt-in setting at any time in the Chrome settings.

Chrome asks your permission before using certain web features (APIs) that might have associated risks. To improve the safety and utility of Chrome permissions, Chrome may anonymously report the domains on which you grant, reject and revoke permissions or ignore or dismiss permission prompts. This happens only if you are a Safe Browsing user and have activated syncing your browsing history and settings with Google without a custom passphrase.

For all Safe Browsing requests and reports, Google logs the transferred data in its raw form and retains this data for up to 30 days. Google collects standard log information for Safe Browsing requests, including an IP address and one or more cookies. After at most 30 days, Safe Browsing deletes the raw logs, storing only calculated data in an anonymized form that does not include your IP addresses or cookies. Additionally, Safe Browsing requests won't be associated with your Google Account. They are, however, tied to the other Safe Browsing requests made from the same device.

Unwanted software protection

The Windows version of Chrome is able to detect and remove certain types of software that violate Google's Unwanted Software Policy. If left in your system, this software may perform unwanted actions, such as changing your Chrome settings without your approval. Chrome periodically scans your device to detect potentially unwanted software. In addition, if you have opted in to automatically report details of possible security incidents to Google, Chrome will report information about unwanted software, including relevant file metadata and system settings linked to the unwanted software found on your computer.

If you perform an unwanted software check on your computer from the Settings page, Chrome reports information about unwanted software and your system. System information includes metadata about programs installed or running on your system that could be associated with harmful software, such as: services and processes, scheduled tasks, system registry values commonly used by malicious software, command-line arguments of Chrome shortcuts, Windows proxy settings, and software modules loaded into Chrome or the network stack. You can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the scan.

If unwanted software is detected, Chrome will offer you an option to remove the software by using the Chrome Cleanup Tool. The Chrome Cleanup Tool also reports information about unwanted software and your system to Google, and again you can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the cleanup.

This data is used for the purpose of improving Google's ability to detect unwanted software and offer better protection to Chrome users. It is used in accordance with Google's Privacy Policy and is stored for up to 14 days, after which only aggregated statistics are retained.

Navigation error tips

Google Chrome can show tips to help guide you to the page you were trying to reach in cases where the web address cannot be found, a connection cannot be made, the server returns a very short (under 512 byte) error message, or you've navigated to a parked domain.

Google Chrome will first check the address against a locally-stored list of suspected parked domains. If there is a match, Chrome sends a partial fingerprint (a hash prefix) of the URL to Google for verification that the domain is indeed parked. This uses the same methodology as the Safe Browsing service (see the "Safe Browsing protection" section, above).

In the case of other navigation errors, the URL of the web page you're trying to reach is stripped of all GET parameters, and then sent to Google in order to retrieve navigation tips. This information is logged and anonymized in the same manner as Google web searches. The logs are used to ensure and improve the quality of the feature.

Additionally, to provide you with more informative error messages when a domain name cannot be found, Chrome will

In the event that Chrome detects SSL connection timeouts, certificate errors, or other network issues that might be caused by a captive portal (a hotel's WiFi network, for instance), Chrome will make a cookieless request to https://www.gstatic.com/generate_204 and check the response code. If that request is redirected, Chrome will open the redirect target in a new tab on the assumption that it's a login page. Requests to the captive portal detection page are not logged.

You can [disable navigation error tips](#) by unchecking the box in the "Privacy" section of Google Chrome's options.

Offline Indicator

On Android versions Lollipop and older, when Chrome detects a network change, it sends a cookieless request to http://connectivitycheck.gstatic.com/generate_204 or http://clients4.google.com/generate_204 to determine whether you're offline and display an offline indicator.

Software updates

Desktop versions of Chrome and the Google Chrome Apps Launcher use [Google Update](#) to keep you up to date with the latest and most secure versions of software. In order to provide greater transparency and to make the technology available to other applications, the Google Update technology is open source.

Google Update requests include information necessary for the update process, such as the version of Chrome, its release channel, basic hardware information, and update errors that have been encountered. The update requests also send Google information that helps us understand [how many people](#) are using Google Chrome and the Chrome Apps Launcher – specifically, whether the software was used in the last day, the number of days since the last time it was used, the total number of days it has been installed, and the number of active profiles. Google Update also periodically sends a non-unique four-letter tag that contains information about [how you obtained Google Chrome](#). This tag is not personally identifiable, does not encode any information about when you obtained Google Chrome, and is the same as everyone who obtained Google Chrome the same way.

Because Chrome OS updates the entire OS stack, Google Update on Chrome OS also sends the current Chrome OS version and hardware model information to Google in order to ensure that the correct software updates and hardware manufacturer customizations such as apps, wallpaper, and help articles are delivered. This information is not personally identifiable, and is common to all users of Chrome OS on the same revision of device.

Unlike the desktop versions of Chrome, the delivery and management of updates for mobile versions of Chrome are managed through the app stores for Android and iOS. Mobile versions of Chrome utilize the servers described above for [counting active installations](#).

Chrome extensions and applications that you've installed are kept up to date with a similar system used for updating desktop versions of Chrome. These update requests include similar information (such as the application ID, when the application was last used, and how long it's been installed). We use these requests to determine the aggregate popularity and usage of applications and extensions. If you are using an extension or application restricted to a certain audience, authentication tokens are sent with the update requests for these add-ons. For security reasons, Chrome also occasionally sends a cookieless request to the Chrome Web Store, in order to verify that installed extensions and applications that claim to be from the store are genuine.

In order to keep updates as small as possible, Google Chrome is internally split into a variety of components, each of which can be updated independently. Each component is uniquely identified via an ID that is shared among all Google Chrome installations (e.g., "fmeadaodfnidclnjhlkdgjkolmhmfofk"). An update request for a component contains this ID, the hash of the previous download (called a "fingerprint"), and the component's version. Because every installation has the same ID, and downloads of the same component have the same fingerprint, none of this information is personally identifiable.

If you install web apps on an Android device, a Google server is responsible for creating a native Android package that can be verified for authenticity by Chrome. When Chrome is updated or notices that the web app's manifest has changed, Chrome asks the server for a new version of the Android package in a cookieless request. If the information needed to create the native Android package cannot be acquired by the server (e.g., because the information is behind a corporate firewall), Chrome sends it to Google and an Android package is created that is unique to you. It contains a unique and random identifier that is not tied to your identity.

Chrome may also download and run a binary executable (e.g., as part of the software update or to improve Safe Browsing protection). These executables are cryptographically signed and verified before execution. Chrome may download further static resources like dictionaries on demand to reduce the size of the installer.

On Windows and OS X versions of Chrome, the recovery component tries to repair Google Update when it's broken. After the relevant binary is executed, Google Update uploads statistics on the actions that were performed. These statistics contain no personally identifiable information.

Network time

On desktop platforms, Chrome uses [network time](#) to verify SSL certificates, which are valid only for a specified time. At random intervals or when Chrome encounters an expired SSL certificate, Chrome may send requests to Google to obtain the time from a trusted source. These requests are more frequent if Chrome believes the system clock is

Counting installations

In order to measure the success rate of Google Chrome downloads and installations of the Windows version of Google Chrome, a randomly-generated token is included with Google Chrome's installer. This token is sent to Google during the installation process to confirm the success of that particular installation. A new token is generated for every install. It is not associated with any personal information, and is deleted once Google Chrome runs and checks for updates the first time.

For Chrome to know how many active installations it has, the mobile version of Chrome sends a ping to Google with a salted hash of a device identifier on an ongoing basis. The desktop version of Chrome does not send any stable identifier to count active installations. Instead an anonymous message to Google with a timestamp of the last ping is used to infer number of active installations.

Measuring effectiveness of a promotion

Chrome utilizes two measurements to understand how effective a promotional campaign has been: how many Chrome installations are acquired through a promotional campaign, and how much Chrome usage and traffic to Google is driven by a campaign.

To measure installations or reactivations of Chrome through a campaign, Chrome will send a token or an identifier unique to your device to Google at the first launch of Chrome, as well as the first search using Google. On desktop versions of Chrome, a token unique to your device is generated. The same token will be sent if Chrome is later reinstalled at first launch and at first use of the Omnibox after reinstallation or reactivation. Rather than storing the token on the computer, it is generated when necessary by using built-in system information that is scrambled in an irreversible manner. On iOS, Chrome uses the IDFA for counting installations acquired by a campaign, and it can be reset in iOS settings.

To measure searches and Chrome usage driven by a particular campaign, Chrome inserts a promotional tag, not unique to you or your device, in the searches you perform on Google. This non-unique tag contains information about how Chrome was obtained, the week when Chrome was installed, and the week when the first search was performed. For desktop versions of Chrome, Chrome generates a promotional tag, if the promotional installation token described in the previous paragraph indicates that Chrome has been installed or reactivated by a campaign on a device which has not been associated with any campaign yet. For Chrome on Mobile, a promotional tag is always sent regardless of the source of installations.

The promotional tag is generated using a software library called "RLZ" and looks similar to "1T4ADBR_enUS236US239". The RLZ library was fully open-sourced in June 2010. For more information, please see the In the Open, for RLZ post on the Chromium blog and the article "How To Read An RLZ String". On Android, this promotional tag can also be a readable string like "android-hms-tmobile-us" instead of an RLZ string, and is not unique to either you or your device.

This non-unique promotional tag is included when performing searches via Google (the tag appears as a parameter beginning with "rlz=" when triggered from the Omnibox, or as an "x-rlz-string" HTTP header). We use this information to measure the searches and Chrome usage driven by a particular promotion.



If usage statistics and crash reports are enabled, the RLZ string is sent along with the report. This allows us to improve Chrome based on variations that are limited to specific geographic regions.

For the desktop version of Chrome, you can opt-out of sending this data to Google by uninstalling Chrome, and installing a version downloaded directly from www.google.com/chrome. To opt-out of sending the RLZ string in Chrome OS, press Ctrl + Alt + T to open the crosh shell, type rlz disable followed by the enter key, and then reboot your device.

Usage statistics and crash reports

Chrome has a feature to automatically send usage statistics and crash reports to Google in order to help improve Chrome's feature set and stability.



Usage statistics contain information such as system information, preferences, user interface feature usage, responsiveness, and memory usage. This feature is enabled by default for Chrome installations of version 54 or later. You can enable or disable the feature in the "Privacy" section of Google Chrome's settings. These statistics do not include any personal information. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs or personal information depending on what was happening at the time of the crash.

When this feature is enabled, Google Chrome stores a randomly generated unique token on your device, which is sent to Google along with your usage statistics and crash reports. The token does not contain any personal information and is used to de-duplicate reports and maintain accuracy in statistics. This token is deleted when the feature is disabled and a new token is regenerated when the feature is enabled again.

Along with usage statistics and crash reports, Chrome also reports anonymous, randomized data that is constructed in a

manner which is not linked to the unique token, and which ensures that no information can be inferred about any particular user's activity. This data collection mechanism is summarized on the [Google research blog](#), and full technical details have been published in a [technical report](#) and presented at the 2014 ACM Computer and Communications Security conference.

Chrome will also anonymously report to Google if requests to websites operated by Google fail or succeed in order to detect and fix problems quickly.

If you are also [syncing](#) your browsing history without a sync passphrase, Chrome usage statistics include information about the web pages you visit and your usage of them. The information will also include the URLs and statistics related to downloaded files. If you sync [extensions](#), these statistics will also include information about the extensions that have been installed from Chrome Web Store. The URLs and statistics are sent along with a unique device identifier that can be reset by turning off history Sync or usage statistics and crash reports. The usage statistics are not tied to your Google account. Google only stores usage statistics associated with published extensions, and URLs that are known by Google's web crawlers. We use this information to improve our products and services, for example, by identifying web pages which load slowly; this gives us insight into how to best improve overall Chrome performance. We also make some statistics available externally, through efforts like the [Chrome User Experience Report](#). Externally published reports are conducted in highly aggregated manner to not reveal individual user's identity.

On iOS, if you are syncing your browsing history without a sync passphrase, Chrome reports usage for certain URLs that other Google apps could open. For example, when you tap on an email address, Chrome presents a dialog that allows you to choose between opening with Google Gmail or other mail apps installed on your device. The usage information also includes which apps were presented to you, which one was selected, and if a Google app was installed. Chrome does not log the actual URL tapped. If you are signed in, this usage is tied to your Google account. If you are signed out, the information is sent to Google with a unique device identifier that can be regenerated by resetting the Google Usage ID found in Chrome settings. The raw reports are deleted within 60 days, after which only the aggregated statistics remain.

Google Surveys in Chrome

When you have "send usage statistics" enabled, you may be randomly selected to participate in surveys to evaluate consumer satisfaction with Chrome features. If you are selected, Chrome on Android requests a survey from Google for you. If a survey is available, Chrome then asks you to answer the survey and submit the responses to Google.

The survey also records basic metrics about your actions, such as time spent looking at the survey and elements that the user clicked. These metrics are sent to Google even if you do not fully complete the survey.

To ensure that surveys are spread evenly across users and not repeatedly served to a single user, the feature stores a randomly generated unique token on the device. This token is used solely for the survey requests and does not contain any personal information. If you disable sending usage statistics, the token will be cleared.

Suggestions for spelling errors

Desktop versions of Chrome can provide smarter spell-checking by sending text you type into the browser to Google's servers, allowing you to apply the same spell-checking technology that's used by Google products like Docs. If this feature is enabled, Chrome sends the entire contents of text fields as you type in them to Google, along with the browser's default language. Google returns a list of suggested spellings that are displayed in the context menu. Cookies are not sent along with these requests. Requests are logged temporarily and anonymously for debugging and quality improvement purposes.

This feature is disabled by default; to turn it on, click "Ask Google for suggestions" in the context menu that appears when you right-click on a misspelled word. You can also turn this feature on or off with the "Use a web service to help resolve spelling errors" checkbox in the Privacy section of Chrome settings. When the feature is turned off, spelling suggestions are generated locally without sending data to Google's servers.

Mobile versions of Chrome rely on the operating system to provide spell-checking.

Translate

Google Chrome's built-in translation feature helps you read more of the Web, regardless of the language of the web page. The feature is enabled by default.



Translation [can be disabled at any time](#) in Chrome's settings.

Language *detection* is done entirely using a client-side library, and does not involve any Google servers. For *translation*, the contents of a web page are only sent to Google if you explicitly decide to translate it by clicking "Translate" on the bar, or if you've previously chosen "Always translate" for a given language via the translate bar Options menu.

If you do choose to translate a web page, the text of that page is sent to [Google Translate](#) for translation. Your cookies are not sent along with that request and the request is sent over SSL. This communication with Google's translation service is covered by the [Google privacy policy](#).

If you've chosen to sync your Chrome history, statistics about the languages of pages you visit and about your

Sign In to Chrome and Sync

Google Chrome provides the option to sign in with your Google Account and synchronize your Chrome data across multiple devices ("Sync"). Synced data can include bookmarks, saved passwords, open tabs, browsing history, extensions and more. In Advanced sync settings, you can choose which types of data to synchronize with this device. By default, all syncable data types are enabled.

On desktop versions of Chrome, signing into or out of any Google web service (e.g. google.com) also signs you into or out of Chrome. You can turn Sync on or off, or adjust which data is syncing, in the "People" section of Chrome settings. If you have turned on Sync and signed out of the account you are syncing to, Sync will pause sending all syncable data to Google until you sign back in with the same account. Some sync data types (such as bookmarks and passwords) that are saved locally while Sync is paused will automatically be synced to your account after you sign back in with the same account.

On mobile versions of Chrome, you can sign into or sign out of Chrome from Chrome settings. Signing into Chrome will also turn on Sync. This can be done for any account that has already been added to the mobile device without authenticating again.

On both desktop and mobile, signing into Chrome keeps you signed into Google web services until you sign out of Chrome. On mobile, signing into Chrome will keep you signed in with all Google Accounts that have been added to the device. On desktop, it will keep you signed in with all Google Accounts that you added from a Google web service, unless you have set "Keep local data only until you quit your browser" in your cookie settings.

On Android and desktop, Chrome signals to Google web services that you are signed into Chrome by attaching an X-Chrome-Connected and/or C-Chrome-ID-Consistency-Request header to any HTTPS requests to Google-owned domains. On iOS, the CHROME_CONNECTED cookie is used instead. This allows those Google web services to update their UI accordingly. If you are using a managed device, your system admin may disable the sign in feature or require that data be deleted when you disconnect your account.

Google uses your personal synchronized data to provide you a consistent browsing experience across your devices, and to customize features in Chrome. You can manage your synchronized history by going to chrome://history in your Chrome browser. If "Include history from Chrome and other apps in your Web & App Activity" is checked on the Web & App Activity controls page, Google also uses your synchronized browsing data to provide personalized Google products and services to you. You can change your preference any time, and manage individual activities associated with your Google account.

The paragraph above describes the use of your personal browsing history. Google also uses aggregated and anonymized synchronized browsing data to improve other Google products and services. For example, we use this information to improve Google Search by helping to detect mobile friendly pages, pages which have stopped serving content, and downloads of malware.

If you would like to use Google's cloud to store and sync your Chrome data without allowing any personalized and aggregated use by Google as described in the previous paragraphs, you can choose to encrypt all of your synced data with a sync passphrase. If you choose this option, it's important to note that Google won't have access to the sync passphrase you set; we won't be able to help you recover data if you forget the passphrase. Regardless of how you choose to encrypt your data, all data is always sent over secure SSL connections to Google's servers.

If you're signed into Chrome and are syncing passwords and/or other types of login credentials without a sync passphrase, these credentials are stored in your Google Account. Chrome may help you sign in with credentials you've saved in Android apps on websites that are associated with the respective apps. Likewise, credentials you've saved for websites can be used to help you sign into related Android apps. You can view the credentials you've saved in Chrome and Android by visiting passwords.google.com in any browser. If you've saved credentials for Android applications, Chrome periodically sends a cookieless request to Google to get an updated list of websites that are associated with those applications. To stop websites and Android apps from automatically signing in using credentials you previously saved, you can turn off Auto Sign-In on passwords.google.com or in Chrome settings under "Manage passwords". For more details see this article.

If you sync your browsing history without a Sync passphrase and your browser's usage statistics and crash reports setting is also enabled, your usage statistics and crash reports will include statistics about the pages you visit. You can read more in the Usage statistics and crash reports section of this Whitepaper.

All data synchronized through Google's servers is subject to Google's Privacy Policy. To get an overview of the Chrome data stored for your Google Account, go to the Chrome section of Google Dashboard. That page also allows you to stop synchronization completely and delete all sync data from Google's servers.

Autofill and Password Management

Google Chrome has a form autofill feature that helps you fill out forms on the web more quickly. Autofill is enabled by default, but it can be turned off at any time in Chrome's settings.

If Autofill is enabled and you encounter a web page containing a form, Chrome sends some information about that form to Google. This information includes a hash of the web page's hostname, as well as form identifiers (such as field names), the basic structure of the form, and Chrome's guess at each field's data type (for example, "field X looks like a

phone number, and field X looks like a country"). This information helps Chrome match up your locally stored Autofill data with the contents of the form, and it also helps to improve the quality of form-filling over time.

If Autofill is enabled when you *submit* a form, Chrome sends the data types you actually used in the form. This information helps Chrome improve its guesses over time. The actual text you typed into the form is not sent to Google.

You can manage your Autofill entries via [Chrome's settings](#), and you can edit or delete saved information at any time. Chrome will never store credit card information without explicit confirmation. If you scan your credit card using a phone camera, the recognition is performed locally.

Chrome may help you sign in to websites with credentials you've saved to Chrome's password manager or Google Smart Lock by autofilling sign-in forms, by offering you an account picker, or by automatically signing you in. You can manage and delete your saved credentials in the "Forms and passwords" section of Chrome's settings. If you enable [password management](#), the same kind of data about forms as described above is sent to Google to interpret password forms correctly and enable Chrome to offer password generation that meets site-specific requirements.

Also, if you choose, you can bring your Autofill data with you to all your Chrome-enabled devices by [syncing it](#) as part of your browser settings (see the "Sign In to Chrome" section of this document). If you choose to sync Autofill information, field values are sent as described in "Sign In to Chrome"; otherwise, field values are not sent.

Payments

If you are signed into Chrome and syncing credit cards and addresses with Google Pay, Chrome will offer to save your credit cards and related billing addresses to Google Pay and on your local device. Integration with Google Pay can be disabled via Chrome's Advanced sync settings. If integration with Google Pay is disabled, credit cards will be saved locally but will not be synced. If integration with Google Pay is enabled, Chrome may offer to autofill forms with credit card data stored in your Google Pay account. The cards from your Google Pay account not already saved locally are masked until you provide the correct CVV code. When providing your CVV code for verification, you can choose to store the credit card locally as part of your Chrome Autofill data. If you choose not to store the card locally, you will be prompted for your CVV code each time you use the card. If you use a card from Google Pay, Chrome will collect information about your computer and share it with Google Pay to prevent fraudulent use of your card.

To delete credit card information saved in Chrome, follow the "Add and edit credit cards" steps in [the Autofill article](#). When you delete a credit card that's also saved in your Google Pay account, you will be redirected to the Google Pay to complete the deletion. After your card has been deleted from your Google Pay account, Chrome will automatically remove that card from your Autofill suggestions.

Chrome also supports the [PaymentRequest API](#) by allowing you to pay for purchases with credit cards from Autofill, Google Pay, and other payment apps already installed on your device. Google Pay and other payment apps are only available on an Android device. PaymentRequest allows the merchant to request the following information: full name, shipping address, billing address, phone number, email, credit card number, credit card expiration, CVV, and Google Pay credentials. Information is not shared with the merchant until you agree.

Geolocation

Google Chrome supports the [Geolocation API](#), which provides access to fine-grained user location information with your consent.

By default, Chrome will request your permission when a web page asks for your location information, and does not send any location information to the web page unless you explicitly consent.

Furthermore, whenever you are on a web page which is using your location information, Chrome will display a location icon on the right side of the omnibox. You can click on this icon in order to find out more information or manage location settings.



In [Chrome's settings](#), by clicking "Show advanced settings.", then clicking "Content Settings" and scrolling to the "Location" section, you can choose to allow all sites to receive your location information, have Chrome ask you every time (the default), or block all sites from receiving your location information. You can also configure exceptions for specific web sites.

In the Android version of Chrome, your default search engine automatically receives your location when you conduct a search. On the iOS version of Chrome, by default your location is sent to Google if you conduct a search from the omnibox. Read more about how your default search engine handles geolocation and how to manage your settings in the [Omnibox](#) section of the [whitepaper](#).

If you do choose to share your location with a web site, Chrome will send local network information to Google (also used by other browsers such as Mozilla Firefox) in order to estimate your location. This local network information can include data about nearby Wi-Fi access points or cellular signal sites/towers (even if you're not using them), and your computer's IP address. The requests are logged, and aggregated and anonymized before being used to operate, support, and improve the overall quality of Google Chrome and Google Location Services.

For further reading on the privacy and user interface implications of the Geolocation API (as well as other HTML5 APIs), see ["Practical Privacy Concerns in a Real World Browser"](#) written by two Google Chrome team members.

Chrome supports the Web Speech API, a mechanism for converting speech to text on a web page. It uses Google's servers to perform the conversion. Using the feature sends an audio recording to Google (audio data is not sent directly to the page itself), along with the domain of the website using the API, your default browser language and the language settings of the website. Cookies are not sent along with these requests.

Google Assistant "Ok Google"

The Google Assistant feature is integrated into some models of Chrome OS devices. If you opt in to the feature, Chrome OS listens for you to say "Ok Google" and sends the audio of the next thing you say, plus a few seconds before, to Google. Detection of the phrase "Ok Google" is performed locally on your computer, and the audio is only sent to Google after it detects "Ok Google". You can enable or disable this feature in Google Assistant Settings.

Enabling this feature in Chrome Settings will cause Chrome to listen whenever the screen is unlocked. On Chrome OS devices with a local audio processor, the device also listens when the device is asleep. On these devices, The Google Assistant feature only works if Voice & Audio Activity is enabled for your Google account. Chrome will prompt you to enable Voice & Audio Activity for the associated Google account if it is disabled.

Once the audio has been converted to text, a search with that text is submitted to Google. If you have used the "Ok Google" search before on a device but turned off Voice & Audio Activity later, your device is still capable of processing your voice and sending the audio to Google but the voice is deleted shortly.

You can determine your Chrome OS device's behavior by examining the text in the "Search and Assistant" section of settings.

Google Cloud Print

The Google Cloud Print feature allows you to print documents from your browser over the Internet. You do not need a direct connection between the machine that executes Chrome and your printer.

If you choose to print a web page via Cloud Print, Chrome will generate a PDF of this website and upload it over an encrypted network connection to Google's servers. If you choose to print other kinds of documents, they may be uploaded as raw documents to Google's servers.

A print job will be downloaded by either a Chrome browser ("Connector") or a Cloud Print capable printer that you selected when printing the website. In some cases the print job must be submitted to a third-party service to print (HP's ePrint, for example).

The print job is deleted from Google's servers when any of three criteria is met:

- You delete the print job
- The job has been printed and marked as printed by the printer/connector
- The job has been queued on Google's servers for 30 days

You can manage your printers and print jobs on the Google Cloud Print website.

SSL certificate reporting

Chrome stores locally a list of expected SSL certificate information for a variety of high-value websites, in an effort to prevent man-in-the-middle attacks. For Google websites and other websites that choose to opt in, Chrome will report a possible attack or misconfiguration. If the certificate provided by the web server doesn't match the expected signature, Chrome reports information about the SSL certificate chain to Google or to a report collection endpoint of the website's choosing. Chrome sends these reports only for certificate chains that use a public root of trust.

Chrome also allows users to choose to send information that helps Google improve SSL warnings and error pages. You can opt in to this feature by checking the box on any SSL error page. While you are opted in, each time you see an SSL error page, a report will be sent to Google's security team. The report contains the SSL certificate chain, the server's hostname, the local time, and relevant details about the validation error and SSL error page type. Because Chrome sends these reports for all certificate chains, even those that chain to a private root of trust, these chains can contain personally identifiable information. You can opt out anytime by unchecking the box "Automatically report details of possible security incidents to Google" in the Privacy section of Chrome's advanced settings.

The SSL certificate reporting feature is not available on Chrome iOS.

Token Binding

Chrome's Token Binding feature allows a server to validate in a strong way that new HTTPS sessions originate from the same client as a previous session. This assertion mitigates the risk of session theft because cookies can be cryptographically tied to a particular Token Binding ID. This feature makes it significantly more difficult to convert stolen cookies into stolen sessions. On the iOS version of Chrome, Token Binding is not used for requests made for web page loading.

Token Binding IDs do not contain any information about the user, and a different Token Binding ID is created for each secure origin. A Token Binding ID created for one server will be shared with another server only if the original server

requests it to be shared. Token Binding IDs are not shared between Chrome profiles, and all Token Binding IDs created during Incognito browsing are destroyed when you exit the Incognito session. Note that Token Bindings are not used for requests that block cookies.

On desktop versions of Chrome, you can determine which Token Binding IDs have been created (and you can remove unwanted IDs) in the Cookies and Site Data dialog (available at <chrome://settings/siteData>). On all platforms, Token Binding IDs are subject to removal when "Cookies and Site Data" are cleared via the "Clear Browsing Data" dialog (<chrome://settings/clearBrowserData>). Token Binding is an evolution of the TLS Channel ID feature.

For more technical details and background information, visit browserauth.net and the work-in-progress [IETF draft](#).

Installed Applications and Extensions

Users can install external apps and extensions for the desktop versions of Chrome to add features to or customize their Chrome browsers. Installing an application or extension from the Chrome Web Store directly or via an [inline installation](#) flow on a third-party site involves a request to the Chrome Web Store for details about the application. This request includes cookies, and if you're logged into Google when you install an application, that installation is recorded as part of your Google account. The store uses this information to recommend applications to you in the future, and in aggregate to evaluate application popularity and usage. As noted above, applications and extensions are updated via Google Update.

As they're more deeply integrated into Chrome, applications and extensions that you choose to install can request access to additional capabilities, enabling functionality that doesn't make sense on the web at large: background notifications or raw socket access, for instance. These additional permissions may change the way your data is collected and shared, as extensions and applications might have access to data regarding the websites you visit, and might be capable of monitoring or modifying your interactions with the web. When installing an application or extension, Chrome may first warn you about [certain capabilities](#). Please do take the time to read and evaluate this warning before proceeding with the installation. Note also that interactions with and data collected by these third-party applications and extensions are governed by their own privacy policies, not Google's privacy policy.

Push messaging

Your device may receive push messages from the backend servers of apps and extensions installed in Chrome, websites that you grant the "notification" permission to, and your default search engine. Disabling push messages from your default search engine is done in the same way as disabling push messages from any site, by visiting the "Notifications" section of "Site settings".

Push message data is sent over a secure channel from the developer through Google's infrastructure to Chrome on your device, which can wake up apps, extensions, and websites (including your default search engine) to deliver the message. The developer may end-to-end encrypt the message data, or may send it in a form such that Google servers process it as plain text. Google servers retain up to 4 weeks' worth of messages to ensure delivery to users even if their devices are offline at the time of the initial pushing.

If the notification permission is set to "granted" for any website (including the default search engine), or you have an app or extension installed that uses push messaging, then Chrome provides the app's, extension's, or website's server with one or more registration tokens that can be used to send messages to the entity (app, extension, or website). Websites you visit in Incognito mode are not allowed to send you push messages and therefore cannot get a registration token.

When you uninstall an app or extension, revoke the notification permission for a website, or clear cookies for a permitted website, its registration token is revoked and will not be reused, even if the same app or extension is re-installed or the same website is re-visited. Registration tokens used by Chrome components such as [Sync](#) are revoked once they are no longer in use (for example, when the user disables Sync). When a registration token is revoked, the associated entity on your device stops receiving messages sent from its developer's server.

The registration tokens that are passed to entities contain an encrypted device ID, which is used for routing the messages. Google can decrypt the device ID, but other entities cannot, and the encryption is designed so that two registration tokens for the same device ID cannot be correlated. On desktop versions of Chrome, the device ID is reset when the Chrome profile is removed (via the "People" section in Chrome's Settings), or when neither Chrome Sync nor any of the entities requires it for push messaging. On Android, the lifetime of the device ID is governed by the operating system and is independent of Chrome. Any messages routed to registration tokens containing a revoked device ID will not be delivered.

Chrome custom tabs

On Android devices, an app developer may use a Custom Tab to show web content when you click on a URL from their app. A Custom Tab may look different from a regular Chrome tab, for example it may have app-specified visual style, and the absence of an editable URL bar. Despite the different visual style a Custom Tab may have, the data sent and received in the Custom Tab, such as cookies, saved passwords and browsing history function the same way they do in a normal Chrome tab. The Custom Tab is an app-customized view using the same underlying user profile.

With Chrome Custom Tabs, an Android app developer may also specify custom actions in the Chrome toolbar and overflow menu that are relevant to their app, for example, "share", "save page", "copy URL". If you tap on such a button, the address of the current website is shared with the application.

An application can request Chrome to pre-render a given URL in the background. This allows Chrome to show you a pre-loaded site instantly when you open it from the app. At the same time it allows an application to set cookies in your browser in the background. To disable pre-rendering, you can uncheck "Prefetch page resources" in the privacy settings.

Continue where you left off

If you have selected the option to "Continue where you left off" in settings on desktop versions of Chrome, when you open Chrome, it attempts to bring you right back to the way things were when the browser was closed. Chrome reloads the tabs you had open and persists session information to get you up and running as quickly as possible. This feature effectively extends a browsing session across restarts. In this mode, session cookies are no longer deleted when the browser closes; instead, they remain available on restart to keep you logged into your favorite sites.

On desktop versions of Chrome, this feature can be enabled or disabled in Chrome settings. On Chrome OS, it is enabled by default.

On OS X, when you restart your device, a checkbox in the OS confirmation dialog asks you whether you want to re-open applications and windows after restart. If you check this box, Chrome restores tabs and windows, as well as the session cookies, even if you have disabled "Continue where you left off" on Chrome.

On mobile versions of Chrome, this feature is always enabled without a setting.

Chrome Variations

We want to build features that users want, so a subset of users may get a sneak peek at new functionality being tested before it's launched to the world at large. A list of field trials that are currently active on your installation of Chrome will be included in all requests sent to Google. This Chrome-Variations header (X-Client-Data) will not contain any personally identifiable information, and will only describe the state of the installation of Chrome itself, including active variations, as well as server-side experiments that may affect the installation.

The variations active for a given installation are determined by a seed number which is randomly selected on first run. If usage statistics and crash reports are disabled, this number is chosen between 0 and 7999 (13 bits of entropy). If you would like to reset your variations seed, run Chrome with the command line flag "--reset-variation-state". Experiments may be further limited by country (determined by your IP address), operating system, Chrome version and other parameters.

Do Not Track

If you enable the "Do Not Track" preference in Chrome's settings, Chrome will send a DNT:1 HTTP header with your outgoing HTTP, HTTPS and SPDY browsing traffic (Chrome cannot, however, guarantee that NPAPI plugins also send the header.) The header will not be sent with system traffic such as the geolocation, metrics or device management services.

The effect of Do Not Track depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example, to improve security; to provide content, services, ads and recommendations on their websites; and to generate reporting statistics.

Chrome on iOS now uses WKWebView to provide a more stable and faster browser. As a result of this move, the Do Not Track preference is no longer available due to iOS constraints. If Apple makes changes to allow this feature, Chrome will make Do Not Track available again in iOS.

Plugins

Chrome ships with an Adobe Flash Player implementation that is based on the Pepper API. Flash and other Pepper-based plugins may ask you for "Access to your computer". If you grant this permission, the plugin is granted unsandboxed access. This allows content providers to offer you access to DRM protected content like videos or music but may have security and privacy implications, so consider carefully whether you trust a plugin or website with this privilege.

Media licenses

Some websites encrypt media to protect against unauthorized access and copying. When users play media from these sites, they typically log into the site, which authenticates the user, and then digital rights management negotiates a key exchange for the decryption and playback of the media.

For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. The implementation of that API is tightly coupled with the browser to protect user privacy and security, through Content Decryption Modules (CDM), which are provided by digital rights management solutions such as Google Widevine or Microsoft PlayReady.

When a user asks Chrome to play encrypted HTML5 media (for example, watching a movie on Google Play Movies), Chrome will generate a request for a license to decrypt that media. This license request contains an automatically generated request ID, which is created by the Content Decryption Module, as well as proof that the CDM is legitimate. After generation, the license request is typically sent to a license server managed by either the content website or Google. Neither the license request, the proof, nor the request ID include any personally identifying information. After

As part of the license request, Chrome also generates a unique session ID which does not contain personally identifying information. This session ID is sent to the license server, and when the server returns a license the session ID is used to decrypt the media. The session ID may be stored locally even after the site has been closed. The license may also be stored locally for offline consumption of protected content. Session ID and licenses may be cleared by the user in Chrome using [Clear Browsing Data](#) with "Media licenses" enabled.

When returning a license, the site license server may include a client ID, generated by the site. This client ID is unique to the user and the site, it is not shared between sites. If provided, the client ID is stored locally and included by Chrome in subsequent license requests to that site. The client ID may be cleared by the user in Chrome using [Clear Browsing Data](#) with "Media licenses" enabled.

On some platforms, the website may additionally request verification that the device is eligible to play specific types of protected content; on Chrome OS, this is known as [Verified Access](#)). In this case, Google creates a certificate using a unique hardware identifier for the device. This hardware ID identifies the device, but does not identify the user. If the user agrees, Google receives the hardware ID and generates a certificate verifying the device for the requested site. The certificate does not include the hardware ID or any other information that could permanently identify the device. Certificates are stored locally similar to other cached browsing data, and may be cleared by the user in Chrome using [Clear Browsing Data](#) with "Media licenses" enabled.

Some sites use Flash instead of HTML5. If a website you visit chooses to use Adobe Flash Access DRM protection, Chrome for Windows and Chrome OS will give Adobe Flash access to a device identifier. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Media licenses" enabled.

In order to give you access to licensed music, the [Google Play Music app](#) can retrieve a device identifier that is derived from your hard drive partitions or, on a Chrome OS or Linux installation, from a unique file on your disk. This identifier can be reset by reinstalling your operating system.

Cloud policy

When you sign into a Chrome OS device, Chrome on Android, or a desktop Chrome profile with an account associated with a Google Apps domain, Chrome checks whether the domain has configured enterprise policies. If so, the Chrome OS user session or Chrome profile is assigned a unique ID, and registered as belonging to that domain. Any configured policies are applied to the profile. In order to revoke the registration, you'll need to remove the Chrome OS user profile, sign out of Chrome on Android, or remove the desktop profile.

Additionally, Chrome OS devices can be enrolled to a Google Apps domain by a domain admin. This will enforce enterprise policies for the entire device, such as providing shared network configurations and restricting access to developer mode. When a Chrome OS device is enrolled to a domain, then a unique device ID is registered to the device. In order to revoke the registration, the admin will need to wipe the entire Chrome OS device.

Registered profiles and devices check for policy changes periodically (every 3 hours by default). In some cases, the server pushes policy changes to the client without waiting for Chrome's periodic check. Unregistered profiles check whether a policy has been turned on for their domain each time Chrome starts up.

The [policy list](#) contains details about the types of configurations that are available via Cloud Policy.

Data Saver

If you enable Data Saver, Chrome will send your traffic through Google's optimizing proxy servers. This option reduces the amount of data downloaded and speeds up your page loads.

Most of the time, only your HTTP traffic is transparently proxied, and you won't notice any changes to the page. However, if Chrome anticipates the page will load especially slowly, both HTTP and HTTPS pages will be optimized to load only the essential content. For HTTPS origins, the transcoded pages are served from a Google-owned domain instead of being transparently proxied. Because these pages are served from a Google-owned domain instead of the original domain, Chrome will not send any origin-scoped information (e.g., cookies or data from local storage) for the original domain to Google, and Google cannot set any origin-scoped information for the original domain in Chrome. Pages loaded in Incognito are never proxied or optimized by Data Saver.

Request URLs are logged, but Cookie and If-None-Match headers are stripped from the logs (and cookies are never seen in the case of HTTPS pages). Additionally, the content of proxied pages is cached but not logged. The logs are not associated with your Google Account, and the entire log entry is removed within 14 days. These logs are also governed by standard Google search logging policies.

Google uses the logged and cached data to improve both Data Saver and Safe Browsing; for example, more effective optimizations can be uncovered by analyzing timing data for pages loaded through the proxy service, and malware can be detected more rapidly by analyzing response data in realtime.

Your IP address is forwarded to the origin HTTP server via an X-Forwarded-For header, in accordance with the HTTP standard. The Data Saver service is a transparent proxy, *not* an anonymization service.

By default, the connection between the browser and the Data Saver proxy is over an encrypted channel. However, a network administrator can [disable](#) the use of an encrypted channel to Data Saver.

If you create a supervised user on Chrome or Chrome OS, certain information such as the supervised user's browsing activity, profile settings and permissions requests for blocked content will be sent to Google in association with your Google Account. You can access the browsing activity of your supervised users at chrome.com/manage. In order to remove data that is associated with a supervised user from Google's servers, please sign in to your Google Account at chrome.com/manage and delete the respective supervised user.

Using Chrome with a kid's Google Account

Chrome for Android offers features to be used when signed in with a [kid's Google Account](#) and automatically signs in a kid's account if they've signed into the Android device. Chrome uses the [Sync feature](#) to sync settings configured by parents to the kid's account. You can read about how Sync data is used in the [Sign in](#) section of this Whitepaper.

The collection and use of Chrome data in association with a kid's Google Account are governed by the [Google Family Link - Children's Privacy Policy](#).

In order for the configured settings to apply to a kid's account, Chrome does not support the following features for a kid's Google Account: signing out of Chrome, [Incognito mode](#), and deleting browsing history from within Chrome. Browsing history can still be removed in the [Chrome section of the Google Dashboard](#).

By default, first party cookie blocking is disabled when Chrome is signed in with a kid's account. Parents can go to chrome.google.com/manage/family to allow their kids to block first party cookies. However, blocking cookies signs kids out of Google web products such as Google Search or YouTube and therefore prevents these products from providing any features designed for kids' Google Accounts.

When Chrome is used with a kid's Google Account, information about the kid's requests to access blocked content is sent to Google and made visible to the kid's parent(s) on chrome.google.com/manage/family and in the [Google Family Link app](#). If the kid's browsing mode is set to "Try to block mature sites", Chrome will send a request to the Google [SafeSearch service](#) for each navigation in order to block access to sites that have been classified as containing mature content.

Incognito and Guest Mode

Incognito mode in Chrome is a temporary browsing mode. It ensures that you don't leave browsing history and cookies on your computer. The browsing history and cookies are deleted only once you have closed the last incognito window. Incognito mode cannot make you invisible on the internet. Websites that you navigate to may record your visits. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Browsing as a Guest in Chrome allows you to use somebody else's computer without modifying their profile. For example, no bookmarks or passwords get stored on their computer. Note that Guest mode does not protect you for example, if the computer you are using is infected by a keylogger that records what you type.

iOS 8 and Mac OS X Yosemite Handoff Support

While browsing in a standard (i.e. non-Incognito) session, Chrome will share your current URL with iOS 8+ to support the Handoff feature that was added in OS X Yosemite. This information is only sent to Apple devices that are paired with your iOS device, and the data is encrypted in transit.

More information is available at [Apple Support](#), [Apple Developers](#), and in the [Apple iOS Security Guide](#). Chrome support for this feature can be disabled in Chrome settings.

Security Key

A FIDO U2F Security Key provides a non-phishable credential which can be used to authenticate a user. This mitigates the risk of various kinds of man-in-the-middle attacks in which websites try to steal your password and use it later.

To prevent abuse, a website is required to be delivered over a secure connection (HTTPS), and to register the security key before it can be used for identification. Once a website is registered with a specific security key, that security key will provide a persistent identifier, regardless of which computer it is plugged into, or whether you're in incognito or guest mode, but you must physically interact with the security key to give a website access to an identifier (by, for example, touching it, or plugging it in).

Physical Web

The Physical Web lets you see a list of URLs being broadcast by objects in the environment around you. Google Chrome looks for Physical Web devices with Bluetooth Low Energy beacons that are broadcasting URLs using the Eddystone protocol. Bluetooth signals can be received from 90 feet away or more, depending on signal strength and the user's environment (although the range is often much shorter, due to obstacles and signal noise). If the Physical Web feature is enabled, Chrome sends detected URLs to Google's Physical Web Service (PWS) via a cookieless HTTPS request. For each URL, the PWS obtains the title of the web page, filters out unsafe results, and returns a ranking based on non-personalized signals about the quality and relevance of the web page.

The Physical Web feature is available on Chrome on iOS and Android. Users will need to turn on Bluetooth to use the feature.

If Android users have location settings enabled on both their device and in Chrome, they will receive a notification the first time they are near a beacon that will give them the option to turn on the Physical Web feature. This beacon's URL is not sent to Google's PWS unless the Physical Web feature is enabled. Users can also enable (or disable) the feature in the Privacy settings. Once a user enables the feature, Chrome scans for nearby devices for a few seconds each time the user unlocks the mobile device in use and sends them to the PWS in order to obtain more information about the beacon. The user receives a silent notification when Chrome finds a nearby URL.

On iOS devices, users can enable (or disable) the feature in the Privacy settings or by adding the Chrome widget to their Today view in the notification center. Additionally, the feature is automatically enabled for users who have location enabled on their device, granted Chrome the location permission, and have granted Google the geolocation permission. Chrome scans for nearby devices whenever it is open in the foreground. When Chrome finds nearby URLs, users will see them as omnibox suggestions. Additionally, Chrome scans for nearby devices for a few seconds when the Today widget is displayed in the notification center.

Bluetooth

Google Chrome supports the Web Bluetooth API, which provides websites with access to nearby Bluetooth Low Energy devices with your consent.

Chrome does not let any page communicate with a device unless you explicitly consent. When a web page asks to pair with a device, Chrome will ask you to choose which device the web page should access, if any. Selecting a device for one page does not give other pages access to the device you have chosen, and does not allow that page to access other devices. Currently, permission for a page to communicate with a device is usually revoked when the page is reloaded, and is always revoked when Chrome is restarted.

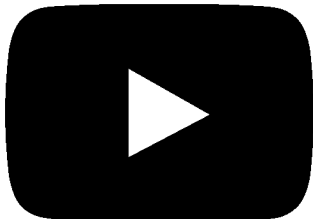
Chrome data that Android sends to Google

The data collection and usage described in this section is handled by Android and governed by the Google Privacy Policy.

If the Android Backup Service is enabled on your device, some of your Chrome preferences will be saved and stored on Google servers. For Nexus and Android One devices, it is described under "Back up your data and settings with Android Backup Service" in this article. For other Android devices, you may be able to find help by looking up your device on this page. When setting up a new Android device, you may request that it copies the preferences from a previously set up device. If you do so, Android may restore backed up Chrome preferences when Chrome is first installed. The new device only copies the preferences if automatic restore is enabled (see "Restore your data and settings" in the same article), Chrome was signed into an account when the backup was made, and the new Android device is signed into that same account.

Chrome's backup data for a particular device may also be restored if you uninstall and then later re-install Chrome on that device. This will only happen if automatic restore is enabled and the device is signed into the account that Chrome was signed into when the backup was made.

Follow us





.



Chrome Family

- [Other Platforms](#)
- [Chromebooks](#)
- [Chromecast](#)
- [Chrome Cleanup Tool](#)



Enterprise

- [Google Chrome Browser](#)
- [Devices](#)
- [Google Cloud](#)
- [G Suite](#)



Education

- [Google Chrome Browser](#)
- [Devices](#)
- [Web Store](#)



Dev and Partners

- [Chromium](#)
- [Chrome OS](#)
- [Chrome Web Store](#)
- [Chrome Experiments](#)
- [Chrome Beta](#)
- [Chrome Dev](#)
- [Chrome Canary](#)



Stay Connected

- [Google Chrome Blog](#)
- [Chrome Help](#)



- [Privacy and Terms](#)
- [About Google](#)
- [Google Products](#)



•

[Help](#)

[Close](#)

Download Chrome for Windows

For Windows 10/8.1/8/7 32-bit.

For Windows 10/8.1/8/7 64-bit.

This computer will no longer receive Google Chrome updates because Windows XP and Windows Vista are no longer supported.

Download Chrome for Mac

For Mac OS X 10.10 or later.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

Download Chrome for Linux

Debian/Ubuntu/Fedora/openSUSE.

Please select your download package:

- ☒ 64 bit .deb (For Debian/Ubuntu)
☐ 64 bit .rpm (For Fedora/openSUSE)

Not Debian/Ubuntu or Fedora/openSUSE? There may be a community-supported version for your distribution [here](#).

Download Chrome for iOS

Google Chrome Terms of Service

These Terms of Service apply to the executable code version of Google Chrome. Source code for Google Chrome is available free of charge under open source software license agreements at <https://code.google.com/chromium/terms.html>.

1.1 Your use of Google's products, software, services and web sites (referred to collectively as the "Services" in this document and excluding any services provided to you by Google under a separate written agreement) is subject to the terms of a legal agreement between you and Google. "Google" means Google Inc., whose principal place of business is at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States. This document explains how the agreement is made up, and sets out some of the terms of that agreement.

1.2 Unless otherwise agreed in writing with Google, your agreement with Google will always include, at a minimum, the terms and conditions set out in this document. These are referred to below as the "Universal Terms". Open source software licenses for Google Chrome source code constitute separate written agreements. To the limited extent that the open source software licenses expressly supersede these Universal Terms, the open source licenses govern your agreement with Google for the use of Google Chrome or specific included components of Google Chrome.

1.3 Your agreement with Google will also include the terms set forth below in the Google Chrome Additional Terms of Service and terms of any Legal Notices applicable to the Services, in addition to the Universal Terms. All of these are referred to below as the "Additional Terms". Where Additional Terms apply to a Service, these will be accessible for you to read either within, or through your use of, that Service.

1.4 The Universal Terms, together with the Additional Terms, form a legally binding agreement between you and Google in relation to your use of the Services. It is important that you take the time to read them carefully. Collectively, this legal agreement is referred to below as the "Terms".

1.5 If there is any contradiction between what the Additional Terms say and what the Universal Terms say, then the Additional Terms shall take precedence in relation to that Service.

2. Accepting the Terms

2.1 In order to use the Services, you must first agree to the Terms. You may not use the Services if you do not accept the Terms.

2.2 You can accept the Terms by:

(A) clicking to accept or agree to the Terms, where this option is made available to you by Google in the user interface for any Service; or

(B) by actually using the Services. In this case, you understand and agree that Google will treat your use of the Services as acceptance of the Terms from that point onwards.

3. Language of the Terms

3.1 Where Google has provided you with a translation of the English language version of the Terms, then you agree that the translation is provided for your convenience only and that the English language versions of the Terms will govern your relationship with Google.

3.2 If there is any contradiction between what the English language version of the Terms says and what a translation says, then the English language version shall take precedence.

4. Provision of the Services by Google

4.1 Google has subsidiaries and affiliated legal entities around the world ("Subsidiaries and Affiliates"). Sometimes, these companies will be providing the Services to you on behalf of Google itself. You acknowledge and agree that Subsidiaries and Affiliates will be entitled to provide the Services to you.

4.2 Google is constantly innovating in order to provide the best possible experience for its users. You acknowledge and agree that the form and nature of the Services which Google provides may change from time to time without prior notice to you.

4.3 As part of this continuing innovation, you acknowledge and agree that Google may stop (permanently or temporarily) providing the Services (or any features within the Services) to you or to users generally at Google's sole discretion, without prior notice to you. You may stop using the Services at any time. You do not need to specifically inform Google when you stop using the Services.

4.4 You acknowledge and agree that if Google disables access to your account, you may be prevented from accessing the Services, your account details or any files or other content which is contained in your account.

5. Use of the Services by you

5.1 You agree to use the Services only for purposes that are permitted by (a) the Terms and (b) any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries).

5.2 You agree that you will not engage in any activity that interferes with or disrupts the Services (or the servers and networks which are connected to the Services).

5.3 Unless you have been specifically permitted to do so in a separate agreement with Google, you agree that you will not reproduce, duplicate, copy, sell, trade or resell the Services for any purpose.

5.4 You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) any breach of your obligations under the Terms and for the consequences (including any loss or damage which Google may suffer) of any such breach.

6. Privacy and your personal information

6.1 For information about Google's data protection practices, please read Google's privacy policy at <https://www.google.com/privacy.html> and at <https://www.google.com/intl/en/chrome/privacy/>. This policy explains how Google treats your personal information, and protects your privacy, when you use the Services.

6.2 You agree to the use of your data in accordance with Google's privacy policies.

7. Content in the Services

7.1 You understand that all information (such as data files, written text, computer software, music, audio files or other sounds, photographs, videos or other images) which you may have access to as part of, or through your use of, the Services are the sole responsibility of the person from which such content originated. All such information is referred to below as the "Content."

7.2 You should be aware that Content presented to you as part of the Services, including but not limited to advertisements in the Services and sponsored Content within the Services may be protected by intellectual property rights which are owned by the sponsors or advertisers who provide that Content to Google (or by other persons or companies on their behalf). You may not modify, rent, lease, loan, sell, distribute or create derivative works based on this Content (either in whole or in part) unless you have been specifically told that you may do so by Google or by the owners of that Content, in a separate agreement.

7.3 Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some of the Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings (see <https://support.google.com/websearch/answer/510?hl=en>). In addition, there are commercially available services and software to limit access to material that you may find objectionable.

7.4 You understand that by using the Services you may be exposed to Content that you may find offensive, indecent or objectionable and that, in this respect, you use the Services at your own risk.

7.5 You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) any Content that you create, transmit or display while using the Services and for the consequences of your actions (including any loss or damage which Google may suffer) by doing so.

8. Proprietary rights

8.1 You acknowledge and agree that Google (or Google's licensors) own all legal right, title and interest in and to the Services, including any intellectual property rights which subsist in the Services (whether those rights happen to be registered or not, and wherever in the world those rights may exist).

8.2 Unless you have agreed otherwise in writing with Google, nothing in the Terms gives you a right to use any of Google's trade names, trade marks, service marks, logos, domain names, and other distinctive brand features.

8.3 If you have been given an explicit right to use any of these brand features in a separate written agreement with Google, then you agree that your use of such features shall be in compliance with that agreement, any applicable provisions of the Terms, and Google's brand feature use guidelines as updated from time to time. These guidelines can be viewed online at <https://www.google.com/permissions/guidelines.html> (or such other URL as Google may provide for this purpose from time to time).

8.4 Google acknowledges and agrees that it obtains no right, title or interest from you (or your licensors) under these Terms in or to any Content that you submit, post, transmit or display on, or through, the Services, including any intellectual property rights which subsist in that Content (whether those rights happen to be registered or not, and wherever in the world those rights may exist). Unless you have agreed otherwise in writing with Google, you agree that you are responsible for protecting and enforcing those rights and that Google has no obligation to do so on your behalf.

8.5 You agree that you shall not remove, obscure, or alter any proprietary rights notices (including copyright and trade mark notices) which may be affixed to or contained within the Services.

8.6 Unless you have been expressly authorized to do so in writing by Google, you agree that in using the Services, you will not use any trade mark, service mark, trade name, logo of any company or organization in a way that is likely or intended to cause confusion about the owner or authorized user of such marks, names or logos.

9. License from Google

9.1 Google gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by Google as part of the Services as provided to you by Google (referred to as the "Software" below). This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Google, in the manner permitted by the Terms.

9.2 Subject to section 1.2, you may not (and you may not permit anyone else to) copy, modify, create a derivative work of, reverse engineer, decompile or otherwise attempt to extract the source code of the Software or any part thereof, unless this is expressly permitted or required by law, or unless you have been specifically told that you may do so by

9.3 Subject to section 1.2, unless Google has given you specific written permission to do so, you may not assign (or grant a sub-license of) your rights to use the Software, grant a security interest in or over your rights to use the Software, or otherwise transfer any part of your rights to use the Software.

10. Content license from you

10.1 You retain copyright and any other rights you already hold in Content which you submit, post or display on or through, the Services.

11. Software updates

11.1 The Software which you use may automatically download and install updates from time to time from Google. These updates are designed to improve, enhance and further develop the Services and may take the form of bug fixes, enhanced functions, new software modules and completely new versions. You agree to receive such updates (and permit Google to deliver these to you) as part of your use of the Services.

12. Ending your relationship with Google

12.1 The Terms will continue to apply until terminated by either you or Google as set out below.

12.2 Google may at any time, terminate its legal agreement with you if:

(A) you have breached any provision of the Terms (or have acted in manner which clearly shows that you do not intend to, or are unable to comply with the provisions of the Terms); or

(B) Google is required to do so by law (for example, where the provision of the Services to you is, or becomes, unlawful); or

(C) the partner with whom Google offered the Services to you has terminated its relationship with Google or ceased to offer the Services to you; or

(D) Google is transitioning to no longer providing the Services to users in the country in which you are resident or from which you use the service; or

(E) the provision of the Services to you by Google is, in Google's opinion, no longer commercially viable.

12.3 Nothing in this Section shall affect Google's rights regarding provision of Services under Section 4 of the Terms.

12.4 When these Terms come to an end, all of the legal rights, obligations and liabilities that you and Google have benefited from, been subject to (or which have accrued over time whilst the Terms have been in force) or which are expressed to continue indefinitely, shall be unaffected by this cessation, and the provisions of paragraph 19.7 shall continue to apply to such rights, obligations and liabilities indefinitely.

13. EXCLUSION OF WARRANTIES

13.1 NOTHING IN THESE TERMS, INCLUDING SECTIONS 13 AND 14, SHALL EXCLUDE OR LIMIT GOOGLE'S WARRANTY OR LIABILITY FOR LOSSES WHICH MAY NOT BE LAWFULLY EXCLUDED OR LIMITED BY APPLICABLE LAW. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR CONDITIONS OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR LOSS OR DAMAGE CAUSED BY NEGLIGENCE, BREACH OF CONTRACT OR BREACH OF IMPLIED TERMS, OR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, ONLY THE LIMITATIONS WHICH ARE LAWFUL IN YOUR JURISDICTION WILL APPLY TO YOU AND OUR LIABILITY WILL BE LIMITED TO THE MAXIMUM EXTENT PERMITTED BY LAW.

13.2 YOU EXPRESSLY UNDERSTAND AND AGREE THAT YOUR USE OF THE SERVICES IS AT YOUR SOLE RISK AND THAT THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE."

13.3 IN PARTICULAR, GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO YOU THAT:

(A) YOUR USE OF THE SERVICES WILL MEET YOUR REQUIREMENTS,

(B) YOUR USE OF THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR,

(C) ANY INFORMATION OBTAINED BY YOU AS A RESULT OF YOUR USE OF THE SERVICES WILL BE ACCURATE OR RELIABLE, AND

(D) THAT DEFECTS IN THE OPERATION OR FUNCTIONALITY OF ANY SOFTWARE PROVIDED TO YOU AS PART OF THE SERVICES WILL BE CORRECTED.

13.4 ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICES IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR OTHER DEVICE OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL.

13.5 NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM GOOGLE OR THROUGH OR FROM THE SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TERMS.

14. LIMITATION OF LIABILITY

14.1 SUBJECT TO OVERALL PROVISION IN PARAGRAPH 13.1 ABOVE, YOU EXPRESSLY UNDERSTAND AND AGREE THAT GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS SHALL NOT BE LIABLE TO YOU FOR:

(A) ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL CONSEQUENTIAL OR EXEMPLARY DAMAGES WHICH MAY BE INCURRED BY YOU, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY.. THIS SHALL INCLUDE, BUT NOT BE LIMITED TO, ANY LOSS OF PROFIT (WHETHER INCURRED DIRECTLY OR INDIRECTLY), ANY LOSS OF GOODWILL OR BUSINESS REPUTATION, ANY LOSS OF DATA SUFFERED, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR OTHER INTANGIBLE LOSS;

(B) ANY LOSS OR DAMAGE WHICH MAY BE INCURRED BY YOU, INCLUDING BUT NOT LIMITED TO LOSS OR DAMAGE AS A RESULT OF:

(I) ANY RELIANCE PLACED BY YOU ON THE COMPLETENESS, ACCURACY OR EXISTENCE OF ANY ADVERTISING, OR AS A RESULT OF ANY RELATIONSHIP OR TRANSACTION BETWEEN YOU AND ANY ADVERTISER OR SPONSOR WHOSE ADVERTISING APPEARS ON THE SERVICES;

(II) ANY CHANGES WHICH GOOGLE MAY MAKE TO THE SERVICES, OR FOR ANY PERMANENT OR TEMPORARY CESSATION IN THE PROVISION OF THE SERVICES (OR ANY FEATURES WITHIN THE SERVICES);

(III) THE DELETION OF, CORRUPTION OF, OR FAILURE TO STORE, ANY CONTENT AND OTHER COMMUNICATIONS DATA MAINTAINED OR TRANSMITTED BY OR THROUGH YOUR USE OF THE SERVICES;

(IV) YOUR FAILURE TO PROVIDE GOOGLE WITH ACCURATE ACCOUNT INFORMATION;

(V) YOUR FAILURE TO KEEP YOUR PASSWORD OR ACCOUNT DETAILS SECURE AND CONFIDENTIAL;

14.2 THE LIMITATIONS ON GOOGLE'S LIABILITY TO YOU IN PARAGRAPH 14.1 ABOVE SHALL APPLY WHETHER OR NOT GOOGLE HAS BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING.

15. Copyright and trade mark policies

15.1 It is Google's policy to respond to notices of alleged copyright infringement that comply with applicable international intellectual property law (including, in the United States, the Digital Millennium Copyright Act) and to terminating the accounts of repeat infringers. Details of Google's policy can be found at <https://www.google.com/dmca.html>.

15.2 Google operates a trade mark complaints procedure in respect of Google's advertising business, details of which can be found at https://www.google.com/tm_complaint.html.

16. Advertisements

16.1 Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.

16.2 The manner, mode and extent of advertising by Google on the Services are subject to change without specific notice to you.

16.3 In consideration for Google granting you access to and use of the Services, you agree that Google may place such advertising on the Services.

17. Other content

17.1 The Services may include hyperlinks to other web sites or content or resources. Google may have no control over any web sites or resources which are provided by companies or persons other than Google.

17.2 You acknowledge and agree that Google is not responsible for the availability of any such external sites or resources, and does not endorse any advertising, products or other materials on or available from such web sites or resources.

17.3 You acknowledge and agree that Google is not liable for any loss or damage which may be incurred by you as a result of the availability of those external sites or resources, or as a result of any reliance placed by you on the completeness, accuracy or existence of any advertising, products or other materials on, or available from, such web sites or resources.

18. Changes to the Terms

18.1 Google may make changes to the Universal Terms or Additional Terms from time to time. When these changes are made, Google will make a new copy of the Universal Terms available at https://www.google.com/intl/en/chrome/privacy/eula_text.html and any new Additional Terms will be made available to you from within, or through, the affected Services.

18.2 You understand and agree that if you use the Services after the date on which the Universal Terms or Additional Terms have changed, Google will treat your use as acceptance of the updated Universal Terms or Additional Terms.

19. General legal terms

19.1 Sometimes when you use the Services, you may (as a result of, or in connection with your use of the Services) use a service or download a piece of software, or purchase goods, which are provided by another person or company. Your use of these other services, software or goods may be subject to separate terms between you and the company or person concerned. If so, the Terms do not affect your legal relationship with these other companies or individuals.

19.2 The Terms constitute the whole legal agreement between you and Google and govern your use of the Services (but excluding any services which Google may provide to you under a separate written agreement), and completely replace any prior agreements between you and Google in relation to the Services.

19.3 You agree that Google may provide you with notices, including those regarding changes to the Terms, by email, regular mail, or postings on the Services.

19.4 You agree that if Google does not exercise or enforce any legal right or remedy which is contained in the Terms (or which Google has the benefit of under any applicable law), this will not be taken to be a formal waiver of Google's rights and that those rights or remedies will still be available to Google.

19.5 If any court of law, having the jurisdiction to decide on this matter, rules that any provision of these Terms is invalid, then that provision will be removed from the Terms without affecting the rest of the Terms. The remaining provisions of the Terms will continue to be valid and enforceable.

19.6 You acknowledge and agree that each member of the group of companies of which Google is the parent shall be third party beneficiaries to the Terms and that such other companies shall be entitled to directly enforce, and rely upon, any provision of the Terms which confers a benefit on (or rights in favor of) them. Other than this, no other person or company shall be third party beneficiaries to the Terms.

19.7 The Terms, and your relationship with Google under the Terms, shall be governed by the laws of the State of California without regard to its conflict of laws provisions. You and Google agree to submit to the exclusive jurisdiction of the courts located within the county of Santa Clara, California to resolve any legal matter arising from the Terms. Notwithstanding this, you agree that Google shall still be allowed to apply for injunctive remedies (or an equivalent type of urgent legal relief) in any jurisdiction.

20. Additional Terms for Extensions for Google Chrome

20.1 These terms in this section apply if you install extensions on your copy of Google Chrome. Extensions are small software programs, developed by Google or third parties, that can modify and enhance the functionality of Google Chrome. Extensions may have greater privileges to access your browser or your computer than regular webpages, including the ability to read and modify your private data.

20.2 From time to time, Google Chrome may check with remote servers (hosted by Google or by third parties) for available updates to extensions, including but not limited to bug fixes or enhanced functionality. You agree that such updates will be automatically requested, downloaded, and installed without further notice to you.

20.3 From time to time, Google may discover an extension that violates Google developer terms or other legal agreements, laws, regulations or policies. Google Chrome will periodically download a list of such extensions from Google's servers. You agree that Google may remotely disable or remove any such extension from user systems in its sole discretion.

21. Additional Terms for Enterprise Use

21.1 If you are a business entity, then the individual accepting on behalf of the entity (for the avoidance of doubt, for business entities, in these Terms, "you" means the entity) represents and warrants that he or she has the authority to act on your behalf, that you represent that you are duly authorized to do business in the country or countries where you operate, and that your employees, officers, representatives, and other agents accessing the Service are duly authorized to access Google Chrome and to legally bind you to these Terms.

21.2 Subject to the Terms, and in addition to the license grant in Section 9, Google grants you a non-exclusive, non-transferable license to reproduce, distribute, install, and use Google Chrome solely on machines intended for use by your employees, officers, representatives, and agents in connection with your business entity, and provided that their use of Google Chrome will be subject to the Terms.

August 12, 2010

Google Chrome Additional Terms of Service

MPEGLA

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PARTNER LICENSED TO PROVIDE AVC

Adobe

Google Chrome may include one or more components provided by Adobe Systems Incorporated and Adobe Software Ireland Limited (collectively "Adobe"). Your use of the Adobe software as provided by Google ("Adobe Software") is subject to the following additional terms (the "Adobe Terms"). You, the entity receiving the Adobe Software, will be hereinafter referred to as "Sublicensee."

1. License Restrictions.

(a) Flash Player, Version 10.x is designed only as a browser plug-in. Sublicensee may not modify or distribute this Adobe Software for use as anything but a browser plug-in for playing back content on a web page. For example, Sublicensee will not modify this Adobe Software in order to allow interoperation with applications that run outside of the browser (e.g., standalone applications, widgets, device UI).

(b) Sublicensee will not expose any APIs of the Flash Player, Version 10.x through a browser plug-in interface in such a way that allows such extension to be used to playback content from a web page as a stand-alone application.

(c) The Chrome-Reader Software may not be used to render any PDF or EPUB documents that utilize digital rights management protocols or systems other than Adobe DRM.

(d) Adobe DRM must be enabled in the Chrome-Reader Software for all Adobe DRM protected PDF and EPUB documents.

(e) The Chrome-Reader Software may not, other than as explicitly permitted by the technical specifications, disable any capabilities provided by Adobe in the Adobe Software, including but not limited to, support for PDF and EPUB formats and Adobe DRM.

2. Electronic Transmission. Sublicensee may allow the download of the Adobe Software from a web site, the Internet, an intranet, or similar technology (an, "Electronic Transmissions") provided that Sublicensee agrees that any distributions of the Adobe Software by Sublicensee, including those on CD-ROM, DVD-ROM or other storage media and Electronic Transmissions, if expressly permitted, shall be subject to reasonable security measures to prevent unauthorized use. With relation to Electronic Transmissions approved hereunder, Sublicensee agrees to employ any reasonable use restrictions set by Adobe, including those related to security and/or the restriction of distribution to end users of the Sublicensee Product.

3. EULA and Distribution Terms.

(a) Sublicensee shall ensure that the Adobe Software is distributed to end users under an enforceable end user license agreement, in favor of Sublicensee and its suppliers containing at least each of the following minimum terms (the "End-User License"): (i) a prohibition against distribution and copying, (ii) a prohibition against modifications and derivative works, (iii) a prohibition against decompiling, reverse engineering, disassembling, and otherwise reducing the Adobe Software to a human-perceivable form, (iv) a provision indicating ownership of Sublicensee Product (as defined in Section 8) by Sublicensee and its licensors, (v) a disclaimer of indirect, special, incidental, punitive, and consequential damages, and (vi) other industry standard disclaimers and limitations, including, as applicable: a disclaimer of all applicable statutory warranties, to the full extent allowed by law.

(b) Sublicensee shall ensure that the Adobe Software is distributed to Sublicensee's distributors under an enforceable distribution license agreement, in favor of Sublicensee and its suppliers containing terms as protective of Adobe as the Adobe Terms.

4. Opensource. Sublicensee will not directly or indirectly grant, or purport to grant, to any third party any rights or immunities under Adobe's intellectual property or proprietary rights that will subject such intellectual property to an open source license or scheme in which there is or could be interpreted to be a requirement that as a condition of use, modification and/or distribution, the Adobe Software be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; or (iii) redistributable at no charge. For clarification purposes, the foregoing restriction does not preclude Sublicensee from distributing, and Sublicensee will distribute the Adobe Software as bundled with the Google Software, without charge.

5. Additional Terms. With respect to any update, upgrade, new versions of the Adobe Software (collectively "Upgrades") provided to Sublicenses, Adobe reserves the right to require additional terms and conditions applicable solely to the Upgrade and future versions thereof, and solely to the extent that such restrictions are imposed by Adobe on all licensees of such Upgrade. If Sublicensee does not agree to such additional terms or conditions, Sublicensee will have no license rights with respect to such Upgrade, and Sublicensee's license rights with respect to the Adobe Software will terminate automatically on the 90th day from the date such additional terms are made available to Sublicensee.

6. Proprietary Rights Notices. Sublicensee shall not, and shall require its distributors not to, delete or in any manner alter the copyright notices, trademarks, logos or related notices, or other proprietary rights notices of Adobe (and its licensors, if any) appearing on or within the Adobe Software or accompanying materials.

7. Technical Requirements. Sublicensee and its distributors may only distribute Adobe Software and/or Upgrade on devices that (i) meet the technical specifications posted on <http://www.adobe.com/mobile/licensees>, (or a successor web site thereto), and (ii) has been verified by Adobe as set forth below.

8. Verification and Update. Sublicensee must submit to Adobe each Sublicensee product (and each version thereof)

containing the Adobe Software and/or Upgrade ("Sublicensee Product") that do not meet the Device Verification exemption criteria to be communicated by Google, for Adobe to verify. Sublicensee shall pay for each submission made by Sublicensee by procuring verification packages at Adobe's then-current terms set forth at <http://flashmobile.adobe.com/>. Sublicensee Product that has not passed verification may not be distributed. Verification will be accomplished in accordance with Adobe's then-current process described at <http://flashmobile.adobe.com/> ("Verification").

9. Profiles and Device Central. Sublicensee will be prompted to enter certain profile information about the Sublicensee Products either as part of the Verification process or some other method, and Sublicensee will provide such information, to Adobe. Adobe may (i) use such profile information as reasonably necessary to verify the Sublicensee Product (if such product is subject to Verification), and (ii) display such profile information in "Adobe Device Intelligence system," located at <https://devices.adobe.com/partnerportal/>, and made available through Adobe's authoring and development tools and services to enable developers and end users to see how content or applications are displayed in Sublicensee Products (e.g. how video images appear in certain phones).

10. Export. Sublicensee acknowledges that the laws and regulations of the United States restrict the export and re-export of commodities and technical data of United States origin, which may include the Adobe Software. Sublicensee agrees that it will not export or re-export the Adobe Software, without the appropriate United States and foreign governmental clearances, if any.

11. Technology Pass-through Terms.

(a) Except pursuant to applicable permissions or agreements therefor, from or with the applicable parties, Sublicensees shall not use and shall not allow the use of, the Adobe Software for the encoding or decoding of mp3 audio only (.mp3) data on any non-pc device (e.g., mobile phone or set-top box), nor may the mp3 encoders or decoders contained in the Adobe Software be used or accessed by any product other than the Adobe Software. The Adobe Software may be used for the encoding or decoding of MP3 data contained within a swf or flv file, which contains video, picture or other data. Sublicensee shall acknowledge that use of the Adobe Software for non-PC devices, as described in the prohibitions in this section, may require the payment of licensing royalties or other amounts to third parties who may hold intellectual property rights related to the MP3 technology and that Adobe nor Sublicensee has not paid any royalties or other amounts on account of third party intellectual property rights for such use. If Sublicensee requires an MP3 encoder or decoder for such use, Sublicensee is responsible for obtaining the necessary intellectual property license, including any applicable patent rights.

(b) Sublicensee will not use, copy, reproduce and modify (i) the On2 source code (provided hereunder as a component of the Source Code) as necessary to enable the Adobe Software to decode video in the Flash video file format (.flv or .f4v), and (ii) the Sorenson Spark source code (provided hereunder as a component of the Source Code) for the limited purpose of making bug fixes and performance enhancements to the Adobe Software. All codecs provided with the Adobe Software may only be used and distributed as an integrated part of the Adobe Software and may not be accessed by any other application, including other Google applications.

(c) The Source Code may be provided with an AAC codec and/or HE-AAC codec ("the AAC Codec"). Use of the AAC Codec is conditioned on Sublicensee obtaining a proper patent license covering necessary patents as provided by VIA Licensing, for end products on or in which the AAC Codec will be used. Sublicensee acknowledges and agrees that Adobe is not providing a patent license for an AAC Codec under this Agreement to Sublicensee or its sublicensees.

(d) THE SOURCE CODE MAY CONTAIN CODE LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR WILL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. See <http://www.mpegla.com>

12. Update. Sublicensee will not circumvent Google's or Adobe's efforts to update the Adobe Software in all Sublicensee's products incorporating the Adobe Software as bundled with the Google Software ("Sublicensee Products").

13. Attribution and Proprietary Notices. Sublicensee will list the Adobe Software in publicly available Sublicensee Product specifications and include appropriate Adobe Software branding (specifically excluding the Adobe corporate logo) on the Sublicensee Product packaging or marketing materials in a manner consistent with branding of other third party products contained within the Sublicensee Product.

14. No Warranty. THE ADOBE SOFTWARE IS MADE AVAILABLE TO SUBLICENSEE FOR USE AND REPRODUCTION "AS IS" AND ADOBE MAKES NO WARRANTY AS TO ITS USE OR PERFORMANCE. ADOBE AND ITS SUPPLIERS DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS OBTAINED BY USING THE ADOBE SOFTWARE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO SUBLICENSEE IN SUBLICENSEE'S JURISDICTION, ADOBE AND ITS SUPPLIERS MAKE NO WARRANTIES, CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING WITHOUT LIMITATION NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, SATISFACTORY QUALITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. SUBLICENSEE AGREES THAT SUBLICENSEE SHALL NOT MAKE ANY WARRANTY, EXPRESS OR IMPLIED, ON BEHALF OF ADOBE.

15. Limitation of Liability. IN NO EVENT WILL ADOBE OR ITS SUPPLIERS BE LIABLE TO SUBLICENSEE FOR ANY DAMAGES, CLAIMS OR COSTS WHATSOEVER OR ANY CONSEQUENTIAL, INDIRECT, OR INCIDENTAL DAMAGES,

OR ANY LOST PROFITS OR LOST SAVINGS, EVEN IF AN ADOBE REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS, DAMAGES, CLAIMS OR COSTS OR FOR ANY CLAIM BY ANY THIRD PARTY. THE FOREGOING LIMITATIONS AND EXCLUSIONS APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW IN SUBLICENSEE'S JURISDICTION. ADOBE'S AGGREGATE LIABILITY AND THAT OF ITS SUPPLIERS UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO ONE THOUSAND DOLLARS (US\$1,000). Nothing contained in this Agreement limits Adobe's liability to Sublicensee in the event of death or personal injury resulting from Adobe's negligence or for the tort of deceit (fraud). Adobe is acting on behalf of its suppliers for the purpose of disclaiming, excluding and/or limiting obligations, warranties and liability as provided in this Agreement, but in no other respects and for no other purpose.

16. Content Protection Terms

(a) Definitions.

"Compliance and Robustness Rules" means the document setting forth compliance and robustness rules for the Adobe Software located at <http://www.adobe.com/mobile/licensees>, or a successor web site thereto.

"Content Protection Functions" means those aspects of the Adobe Software that are designed to ensure compliance with the Compliance and Robustness Rules, and to prevent playback, copying, modification, redistribution or other actions with respect to digital content distributed for consumption by users of the Adobe Software when such actions are not authorized by the owners of such digital content or its licensed distributors.

"Content Protection Code" means code within certain designated versions of the Adobe Software that enables certain Content Protection Functions.

"Key" means a cryptographic value contained in the Adobe Software for use in decrypting digital content.

(b) License Restrictions. Sublicensee's right to exercise the licenses with respect to the Adobe Software is subject to the following additional restrictions and obligations. Sublicensee will ensure that Sublicensee's customers comply with these restrictions and obligations to the same extent imposed on Sublicensee with respect to the Adobe Software; any failure by Sublicensee's customers to comply with these additional restrictions and obligations shall be treated as a material breach by Sublicensee.

b.1. Sublicensee and customers may only distribute the Adobe Software that meets the Robustness and Compliance Rules as so confirmed by Sublicensee during the verification process described above in the Adobe Terms.

b.2. Sublicensee shall not (i) circumvent the Content Protection Functions of either the Adobe Software or any related Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software or (ii) develop or distribute products that are designed to circumvent the Content Protection Functions of either the Adobe Software or any Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software.

(c) The Keys are hereby designated as Adobe's Confidential Information, and Sublicensee will, with respect to the Keys, adhere to Adobe's Source Code Handling Procedure (to be provided by Adobe upon request).

(d) Injunctive Relief. Sublicensee agrees that a breach of this Agreement may compromise the Content Protection Functions of the Adobe Software and may cause unique and lasting harm to the interests of Adobe and owners of digital content that rely on such Content Protection Functions, and that monetary damages may be inadequate to compensate fully for such harm. Therefore, Sublicensee further agrees that Adobe may be entitled to seek injunctive relief to prevent or limit the harm caused by any such breach, in addition to monetary damages.

17. Intended Third-party Beneficiary. Adobe Systems Incorporated and Adobe Software Ireland Limited are the intended third-party beneficiaries of Google's agreement with Sublicensee with respect to the Adobe Software, including but not limited to, the Adobe Terms. Sublicensee agrees, notwithstanding anything to the contrary in its agreement with Google, that Google may disclose Sublicensee's identity to Adobe and certify in writing that Sublicensee has entered into a license agreement with Google which includes the Adobe Terms. Sublicensee must have an agreement with each of its licensees, and if such licensees are allowed to redistribute the Adobe Software, such agreement will include the Adobe Terms.

Printer-friendly version

Note: Installing Google Chrome will **add the Google repository** so your system will automatically keep Google Chrome up to date. If you don't want Google's repository, do "sudo touch /etc/default/google-chrome" before installing the package.

☒ Set Google Chrome as my default browser

☒ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. [Learn more](#)

Accept and Install 

Download Chrome

Download for Windows

For Windows 10/8.1/8/7 32-bit

This computer will no longer receive Google Chrome updates because Windows XP and Windows Vista are no longer supported.

[Download for Mac](#)

Mac OS X 10.10 or later

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

[Download for Linux](#)

Debian/Ubuntu/Fedora/openSUSE

Download for phone or tablet

- [Android](#)
- [iOS](#)

Download for another desktop OS

- [Windows 10/8.1/8/7 64-bit](#)
- [Windows 10/8.1/8/7 32-bit](#)
- [Mac OS X 10.10 or later](#)
- [Linux](#)

Frozen versions

- [Windows XP](#)
- [Windows Vista](#)
- [Mac 10.6 - 10.8](#)
- [Mac 10.9](#)

EXHIBIT 24



Go g e

[Chrome](#)

[Skip to content](#)

- [Do More with Chrome](#)
- [Extensions](#)
- [Enterprise](#)

Download [Chrome](#)

Go g e

[Chrome](#)

- [Do More with Chrome](#)
- [Extensions](#)
- [Enterprise](#)

Google Chrome Privacy Whitepaper

Last modified: November 11, 2018 (Current as of Chrome 70.0.3538)

- [Omnibox](#)
- [Network predictions](#)
- [Search locale](#)
- [New Tab page](#)
- [Tap to Search](#)
- [More like this](#)
- [Safe Browsing protection](#)
- [Unwanted software protection](#)
- [Navigation errors](#)
- [Offline Indicator](#)
- [Google update](#)
- [Network time](#)
- [Counting install](#)
- [Measuring promotions](#)
- [Usage stats](#)
- [Google Surveys](#)
- [Spelling suggestions](#)
- [Translate](#)
- [Signing In](#)
- [Autofill](#)
- [Payments](#)
- [Geolocation](#)
- [Speech to text](#)
- [Google Assistant](#)
- [Cloud Print](#)
- [SSL certificate error reporting](#)
- [Token Binding](#)
- [Installed apps](#)
- [Push Messaging](#)
- [Chrome custom tabs](#)
- [Continue where you left off](#)

- [Chrome variations](#)
- [Do Not Track](#)
- [Plugins](#)
- [Media licenses](#)
- [Cloud policy](#)
- [Data Saver \(Chrome mobile\)](#)
- [Supervised users](#)
- [Kid's Google Account](#)
- [Incognito and Guest mode](#)
- [Handoff support](#)
- [Security key](#)
- [Physical web](#)
- [Bluetooth](#)
- [Data sent by Android](#)

This document describes the features in Chrome that communicate with Google, as well as with third-party services (for example, if you've changed your default search engine). This document also describes the controls available to you regarding how your data is used by Chrome. Here we're focusing on the desktop version of Chrome; we touch only tangentially on Chrome OS and Chrome for Mobile. This document does not cover features that are still under development, such as features in the beta, dev and canary channel and active field trials, or Android apps on Chrome OS if Play Apps are enabled.

If you have questions about Google Chrome and Privacy that this document doesn't answer, please contact the privacy team at privacy@chromium.org. We'd be happy to hear from you.

Redesigned Sync and Google service settings

In version 69, we will begin rolling out a new structure for Chrome settings for a small population of users. All settings that control how Google collects data from Chrome have been moved to a new settings page titled "Sync and Google services," combining previous settings from the "Sync" and "Privacy" section of advanced settings.

Additionally, two new data collection settings have been added to this settings page to control when URL-keyed data is collected by Google: "Activity and interactions" and "Make searches and browsing better (Sends URLs of pages you visit to Google)."

"Activity and interactions" controls the collection of URL-keyed data tied to the user's Google Account (for signed in users) for personalization. For example, the URL of the page you are viewing is sent to Google in order to provide better, contextually relevant suggestions in the Omnibox if "Activity and interactions" is turned on and Google is your default search engine. Previously, this URL was sent if history sync was turned on without a custom passphrase.

"Make searches and browsing better" controls the collection of anonymous URL-keyed data that is used to improve Chrome and the user's general browsing experience. For example, Chrome usage statistics include information about the web pages you visit and your usage of them if "Make searches and browsing better" is turned on. Previously, this data was included if history sync was turned on without a custom passphrase.

Both of these settings allow the user to turn off collection of URL-keyed data without turning off the history sync feature.

Finally, users in this population will also see a modified Chrome sync opt-in dialogue. This new version includes language to cover all Google services on the newly revised "Sync and Google services" settings page, including the two new settings controlling collection of URL-keyed data. When the user accepts the new opt-in dialogue, all of these settings are turned on. The user can click "Settings" from the opt-in dialogue to configure exactly which settings they want turned on.

Omnibox

Google Chrome uses a combined [web address and search bar](#) (we call it the "omnibox") at the top of the browser window.

As you use the omnibox, your [default search engine](#) can suggest addresses and search queries that may be of interest to you. These suggestions make navigation and searching faster and easier, and are turned on by default. They can be turned off by unchecking "Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box" in the "Privacy" section of Chrome's settings. They are also disabled in incognito mode.



In order to provide these suggestions, Chrome sends the text you've typed into the omnibox, along with a general categorization (e.g., "URL", "search query", or "unknown"), to your default search engine. Chrome will also send a signal to your default search provider when you focus in the omnibox, telling it to get ready to provide suggestions. Your IP address and certain cookies are also sent to your default search engine with all requests, in order to return the results that are most relevant to you.

If Chrome determines that your typing may contain sensitive information, such as authentication credentials, local file names, or URL data that is normally encrypted, it will not send the typed text.

If Google is your default search engine, when you select one of the omnibox suggestions, Chrome sends your original

search query, the suggestion you selected, and the position of the suggestion back to Google. This information helps improve the quality of the suggestion feature, and it's logged and anonymized in the same manner as Google web searches. Logs of these suggestion requests are retained for two weeks, after which 2% of the log data is randomly selected, anonymized, and retained in order to improve the suggestion feature.

If you've chosen to sync your Chrome history, and if Google is your default search engine, the URL of the page you're viewing is sent to Google in order to provide better, contextually relevant suggestions. URLs are sent only for HTTP pages and HTTPS pages, not other schemes such as file: and ftp:. Additionally, Chrome may present suggestions as soon as you place the cursor in the omnibox, before you start typing. Chrome is in the process of transitioning to a new service to provide these on-focus suggestions. For most users on desktop versions of Chrome, the request and complete set of suggestions are retained on Google servers in order to further improve and personalize the feature. When the URL that triggered the set of suggestions is deleted from your history, the set of suggestions will stop influencing suggestions personalized to you, and will be deleted; otherwise they are retained in your Google account for a year. For a small portion of users on desktop versions of Chrome, and users on mobile versions of Chrome, the logging described in the previous paragraphs apply except that URLs are never included in the 2% sampling of log data.

On Android, your location will also be sent to Google via an X-Geo HTTP request header if Google is your default search engine, the Chrome app has the permission to use your geolocation and you haven't blocked geolocation for www.google.com (or country-specific origins such as www.google.de). Additionally, if your device has network location enabled (High Accuracy or Battery Saving Device Location mode in Android settings), the X-Geo header may also include visible network IDs (WiFi and Cell), used to geocode the request server-side. The X-Geo header will never be sent in Incognito mode. HTTPS will be required to include this header in the request. You can learn more about how to control the Android OS location sharing with apps on [this article](#) for Nexus, or find your device [here](#) if you do not use a Nexus. How to control location sharing with a site within Chrome is written in [this article](#). See the [Geolocation](#) section of this whitepaper for more information on default geolocation permissions.

Additionally, if Google is your search engine and you have enabled sync, omnibox may also show suggestions for your Google Drive files. You can turn this functionality off by disabling the "Drive suggestions" option in Sync settings.

If you use a non-Google search provider as your default search engine, queries are sent and logged under that provider's privacy policy.

Additionally, when you use the omnibox to search for a single word, Chrome may send this word to your DNS server to see whether it corresponds to a host on your network, and may try to connect to the corresponding host. This gives you the option to navigate to that host instead of searching. For example, if your router goes by the hostname "router", and you type "router" in the omnibox, you're given the option to navigate to <https://router/>, as well as to search for the word "router" with your default search provider. This feature is not controlled by the "Use a prediction service to help complete searches and URLs..." option because it does not involve sending data to your default search engine.

Network predictions

Chrome uses a prediction service to load pages more quickly. The prediction service uses navigation history and local heuristics to predict which resources and pages are likely to be needed next, and it initiates actions such as DNS prefetching, TCP and TLS preconnection, and prefetching of web pages. To [turn off](#) network predictions, uncheck "Use a prediction service to load pages more quickly" in the "Privacy" section of Chrome's settings.

To improve load times, the browser can be asked to prefetch links that you might click next. Chrome supports four types of prefetching:

- Chrome prefetching - can be initiated by Chrome itself whenever it detects a search query typed in the omnibox or a likely beginning of a URL you type often
- Webpage prefetching - requested by one web page to prefetch another
- AMP prefetching - can be requested only by the Google Search App on Android to prefetch several accelerated mobile pages (AMP) articles and display them later in a Chrome Custom Tab
- CustomTabs prefetching - any Android app can request to prefetch several URLs to speed up displaying them later in a Chrome Custom Tab

Controlling the feature. All prefetching types except webpage prefetching are controlled by Chrome's prediction service setting. Webpage prefetching is allowed regardless of whether Chrome's network prediction service feature is enabled.

Handling of cookies. The prefetched site is allowed to set and read its own cookies just as if you had visited it (even if you don't end up visiting the prefetched page). All types of prefetching are disabled if you disallow third party cookies to prevent cookies from being set from pages that you did not visit.

Javascript execution. For AMP prefetching the page is fully rendered and Javascript is also executed. For the remaining types of prefetching Javascript is not executed.

Google search locale

If Google is set as your default search engine, Chrome will try to determine the most appropriate locale for Google search queries conducted from the [omnibox](#) in order to give you relevant search results based on your location. For example, if you were in Germany, your omnibox searches may go through google.de instead of google.com.

In order to do this, Chrome will send a request to google.com each time you start the browser. If you already have any cookies from the google.com domain, this request will also include these cookies, and is logged as any normal HTTPS

New Tab page

The Chrome New Tab page may display suggestions for websites that you might want to visit.

In order to help you get started, Chrome may suggest content that is popular in your country or region. Chrome uses your IP address to identify your country or region.

Chrome tries to make personalized suggestions that are useful to you. For this, Chrome uses the sites you have visited from your local browsing history. The most popular languages of the sites you visited may also be sent to Google to provide suggestions in languages you prefer to read.

If you are signed into Chrome, suggestions are *also* based on data stored in your Google account activity. You can control the collection of data in your Google account at [Activity controls](#) and manage your account activity at [My Activity](#). For example, if you sync your browsing history and have enabled its use in your Web & App activity, Google may suggest sites that relate to sites you have visited in the past. Chrome measures the quality of suggestions by sending Google information about the sets of suggestions that were displayed, and those that were selected.

On the desktop version of Chrome, you may also manually add shortcuts to websites that you regularly visit, or edit Chrome's existing website suggestions. After you add, edit, or delete a shortcut to a website, the Chrome New Tab page will not suggest any new websites to you.

Suggestions generated from your browsing history will be removed once you clear your browsing history. However, if you customized your suggestions, they will not be removed.

For Chrome on Android, in certain countries, Chrome may download the content of the New Tab page suggestions from Google, for use while offline. Chrome sends to Google a cookieless request with the URL for each suggestion, along with Chrome's user agent string, in order to render the content. You can remove downloaded content by clearing Chrome's cache data, or by opening the Downloads menu and [selecting individual pages to delete](#). You can disable this feature by disabling "Automatically download pages" in Chrome's Privacy settings.

For desktop and Android versions of Chrome, when you open a new tab, Chrome loads a New Tab page customized by your default search engine (e.g., google.com) if it's available. This page is preloaded in the background and refreshed periodically so that it opens quickly. Your IP address and cookies, as well as your current browser theme, are sent to your search engine with each refresh request so that the New Tab page can be correctly displayed. See the [Embedded Search API](#) for more details. Your search engine may also record your interactions with the New Tab page.

The New Tab page content may be designed by your default search provider. Suggested websites are embedded by Chrome into the New Tab page in a way that does not expose them to your default search provider.

This information about the New Tab page may not apply if you've installed an extension that [overrides the New Tab page](#).

Tap to Search

If you've enabled "Tap to Search" on Chrome Mobile you can search for terms by tapping them.

When you tap a word, the word, the surrounding text, and the home country of your device's SIM card are sent to Google to identify recommended search terms (for example, tapping on "Michael" on a site about Michael Jackson might lead to a suggested search for "Michael Jackson"). The tapped word is logged in accordance with standard Google logging policies, and the surrounding text and home country are logged only when the page is already in Google's search index. If you sync your browsing history, the URL of the page is also sent and logged, and is used to improve your query suggestions.

When Google returns a search suggestion, a card "peeks through" at the bottom of the screen, showing the suggested search term. Opening this card is considered a regular search and navigation on Google, so standard logging policies apply.

Long-pressing on a word opens a peeking card with the selected word, except on recent versions of [Android Oreo](#) and higher which activates Smart Text Selection instead. No communication with Google occurs until the card is opened, and no surrounding text is sent. Saying "Ok Google" after long-pressing on a word provides the word and its surrounding text as context for the Google Assistant.

Tap to Search is enabled in a limited mode by default: potentially privacy-sensitive data, such as the URL and surrounding text, is not sent for HTTPS pages. Tap to Search can be fully enabled and disabled in the card or in the Chrome privacy settings.

More like this

If you have chosen to sync your browsing history, Chrome may provide contextually relevant content recommendations on certain pages via a "More like this" button on the top toolbar and the suggestions will be shown from a bottom sheet.

In order to provide these suggestions, the URL of the page that you're currently viewing, along with your language or locale information and IP address is sent to Google. Suggestions are only fetched for HTTP and HTTPS pages, not pages

Suggestions are not available on all webpages. When there are suggestions, the “More like this” button will appear on the top toolbar.

Safe Browsing protection

Google Chrome includes an optional feature called “Safe Browsing” to help protect you against phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. You can find more information at safebrowsing.google.com about how Safe Browsing protects you in Chrome and other Google products. Safe Browsing is designed specifically to protect your privacy and is also used by other popular browsers. This feature is not available on the iOS version of Chrome.

When Safe Browsing is enabled in Chrome, Chrome contacts Google's servers periodically to download the most recent Safe Browsing list of unsafe extensions and sites, including phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. The most recent copy of this list is stored locally on your system. Chrome checks the URL of each site you visit or file you download against this local list. If you navigate to a URL that appears on the list, Chrome sends a partial URL fingerprint (the first 32 bits of a SHA-256 hash of the URL) to Google for verification that the URL is indeed dangerous. Chrome also sends a partial URL fingerprint when a site requests a potentially dangerous permission, so that Google can protect you if the site is malicious. Google cannot determine the actual URL from this information.

In addition to the URL check described above, Chrome also conducts client-side checks. If a website looks suspicious, Chrome sends a subset of likely phishing and social engineering terms found on the page to Google, in order to determine whether the website should be considered malicious. Chrome can also help protect you from phishing if you type one of your previously saved passwords into an uncommon site. In this case Chrome sends the URL and referrers of the page to Google to see if the page might be trying to steal your password.

If you encounter a website that is on Chrome's Safe Browsing list, you may see a warning like the one shown below. From there, you can choose to opt in to reporting data relevant to security to help improve Safe Browsing and security on the Internet. If you opt in, an incident report will be sent every time you receive a warning or visit a suspicious page. Chrome is currently transitioning this opt-in to change the reporting functionality. If your checkbox reads “Automatically send some system information and page content to Google to help detect dangerous apps and sites” then you are part of the new group of users. This setting differs from the old “report security incidents to Google” in that security reports will also be sent on a very small sample of other sites to help Safe Browsing learn about new threats you may be encountering. This new setting will be unchecked by default even if you opted in to the older setting. The reports are sent to Google over an encrypted channel and can include URLs, headers, and snippets of content from the page and they never include data from browsing you do in Incognito mode. In cases where Chrome discovers unwanted or malicious software on your machine, the reports may also include details about malicious files and registry entries. This data is used only to improve Safe Browsing and to improve security on the Internet. For example, Chrome reports some SSL certificate chains to Google to help improve the accuracy of Chrome's SSL warnings.



You can [visit our malware warning test page](#) or [social engineering warning test page](#) to see the above example in action. For more information about the warning pages, see [Manage warnings about unsafe sites](#). You can find settings for Safe Browsing and the additional reports in the Privacy section of Chrome settings. Please be aware that if you disable the Safe Browsing feature, Chrome will no longer be able to protect you from websites that try to steal your information or install harmful software. We don't recommend turning it off.

If you are a webmaster, developer, or network admin, you can find more relevant information about Safe Browsing on [this page](#).

Safe Browsing also protects you from abusive extensions and malicious software. At start up of Chrome, Safe Browsing scans extensions installed in your browser against the Safe Browsing list. If an extension on the list is found, Chrome will temporarily disable the extension, offer you relevant information and provide an option for you to remove the extension or re-enable it. Chrome also sends the particular extension ID to Safe Browsing. If you attempt to download a file on Chrome's Safe Browsing list, you'll see a warning like this one:



To warn you about potentially dangerous files, like the picture shown above, Chrome checks the URL of potentially dangerous file types you download against a list of URLs that have been verified. This list is stored locally on your computer and updated regularly. Chrome does not send information to Google for files you download from URLs in this list, or if the file is signed by a verified publisher. For all other unverified potentially dangerous file downloads, Chrome sends Google the information needed to help determine whether the download is harmful, including some or all of the following: information about the full URL of the site or file download, all related referrers and redirects, code signing certificates, file hashes, and file header information. Chrome may then show a warning like the one pictured above.

Chrome helps protect you against password phishing by checking with Google when you enter your password on an uncommon page. Chrome keeps a local list of popular websites that Safe Browsing found to be safe. If Chrome detects that you have entered your Google account password or one of your passwords stored in Chrome's password manager on a website that's not on the list, it sends a request to Safe Browsing to gather the reputation of that website. The verdict received from Safe Browsing is usually cached on your device for 1 week.

If the reused password is your Google account password and the verdict for the website is that it is phishing, Chrome will suggest that you change your Google account password to avoid losing access to your account. Additionally, if you sync your browsing history without a sync passphrase, Chrome sends another request to tell Google that your password was likely phished, to make hijacking of your Google account by an adversary more difficult. The information sent in this request includes the ID of the synced browsing history entry to identify the URL where the phishing attempt happened, and the verdict received from Safe Browsing.

If you've opted into sharing data relevant to security to help detect dangerous apps and sites, Chrome also sends a request to Safe Browsing each time you start to enter a password on a page that isn't in Chrome's local list. In addition, the request that Chrome sends to Safe Browsing to determine the reputation of the website on which you reuse your password includes the list of websites for which you saved this password in Chrome's password manager (but not the password itself).

If Chrome suspects that your settings have been tampered with, Chrome reports the URL of the last downloaded potentially dangerous file, and information about the nature of the possible tampering, to the Safe Browsing service.

For some downloads, Chrome may ask you to opt in to reporting to Google Safe Browsing some data relevant to security, in order to improve the quality of download protection. Once you've opted in, some downloaded files that are suspicious will be sent to Google for investigation each time they are encountered. You can change this opt-in setting at any time in the Chrome settings.

Chrome asks your permission before using certain web features (APIs) that might have associated risks. To improve the safety and utility of Chrome permissions, Chrome may anonymously report the domains on which you grant, reject and revoke permissions or ignore or dismiss permission prompts. This happens only if you are a Safe Browsing user and have activated syncing your browsing history and settings with Google without a custom passphrase.

For all Safe Browsing requests and reports, Google logs the transferred data in its raw form and retains this data for up to 30 days. Google collects standard log information for Safe Browsing requests, including an IP address and one or more cookies. After at most 30 days, Safe Browsing deletes the raw logs, storing only calculated data in an anonymized form that does not include your IP addresses or cookies. Additionally, Safe Browsing requests won't be associated with your Google Account. They are, however, tied to the other Safe Browsing requests made from the same device.

Unwanted software protection

The Windows version of Chrome is able to detect and remove certain types of software that violate Google's Unwanted Software Policy. If left in your system, this software may perform unwanted actions, such as changing your Chrome settings without your approval. Chrome periodically scans your device to detect potentially unwanted software. In addition, if you have opted in to automatically report details of possible security incidents to Google, Chrome will report information about unwanted software, including relevant file metadata and system settings linked to the unwanted software found on your computer.

If you perform an unwanted software check on your computer from the Settings page, Chrome reports information about unwanted software and your system. System information includes metadata about programs installed or running on your system that could be associated with harmful software, such as: services and processes, scheduled tasks, system registry values commonly used by malicious software, Windows proxy settings, and software modules loaded into Chrome or the network stack. You can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the scan.

If unwanted software is detected, Chrome will offer you an option to remove the software by using the Chrome Cleanup Tool. The Chrome Cleanup Tool also reports information about unwanted software and your system to Google, and again you can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the cleanup.

This data is used for the purpose of improving Google's ability to detect unwanted software and offer better protection to Chrome users. It is used in accordance with Google's Privacy Policy and is stored for up to 14 days, after which only aggregated statistics are retained.

Navigation error tips

Google Chrome can show tips to help guide you to the page you were trying to reach in cases where the web address cannot be found, a connection cannot be made, the server returns a very short (under 512 byte) error message, or you've navigated to a parked domain.

Google Chrome will first check the address against a locally-stored list of suspected parked domains. If there is a match, Chrome sends a partial fingerprint (a hash prefix) of the URL to Google for verification that the domain is indeed parked. This uses the same methodology as the Safe Browsing service (see the "Safe Browsing protection" section, above).

In the case of other navigation errors, the URL of the web page you're trying to reach is stripped of all GET parameters, and then sent to Google in order to retrieve navigation tips. This information is logged and anonymized in the same manner as Google web searches. The logs are used to ensure and improve the quality of the feature.

Additionally, to provide you with more informative error messages when a domain name cannot be found, Chrome will investigate the underlying cause by attempting to resolve "google.com" using both Google Public DNS and the default DNS service configured for your system.

In the event that Chrome detects SSL connection timeouts, certificate errors, or other network issues that might be caused by a captive portal (a hotel's WiFi network, for instance), Chrome will make a cookieless request to https://www.gstatic.com/generate_204 and check the response code. If that request is redirected, Chrome will open the redirect target in a new tab on the assumption that it's a login page. Requests to the captive portal detection page are not logged.

You can [disable navigation error tips](#) by unchecking the box in the "Privacy" section of Google Chrome's options.

Offline Indicator

On Android versions Lollipop and older, when Chrome detects a network change, it sends a cookieless request to http://connectivitycheck.gstatic.com/generate_204 or http://clients4.google.com/generate_204 to determine whether you're offline and display an offline indicator.

Software updates

Desktop versions of Chrome and the Google Chrome Apps Launcher use [Google Update](#) to keep you up to date with the latest and most secure versions of software. In order to provide greater transparency and to make the technology available to other applications, the Google Update technology is open source.

Google Update requests include information necessary for the update process, such as the version of Chrome, its release channel, basic hardware information, and update errors that have been encountered. The update requests also send Google information that helps us understand [how many people](#) are using Google Chrome and the Chrome Apps Launcher – specifically, whether the software was used in the last day, the number of days since the last time it was used, the total number of days it has been installed, and the number of active profiles. Google Update also periodically sends a non-unique four-letter tag that contains information about [how you obtained Google Chrome](#). This tag is not personally identifiable, does not encode any information about when you obtained Google Chrome, and is the same as everyone who obtained Google Chrome the same way.

Because Chrome OS updates the entire OS stack, Google Update on Chrome OS also sends the current Chrome OS version and hardware model information to Google in order to ensure that the correct software updates and hardware manufacturer customizations such as apps, wallpaper, and help articles are delivered. This information is not personally identifiable, and is common to all users of Chrome OS on the same revision of device.

Unlike the desktop versions of Chrome, the delivery and management of updates for mobile versions of Chrome are managed through the app stores for Android and iOS. Mobile versions of Chrome utilize the servers described above for [counting active installations](#).

Chrome extensions and applications that you've installed are kept up to date with a similar system used for updating desktop versions of Chrome. These update requests include similar information (such as the application ID, when the application was last used, and how long it's been installed). We use these requests to determine the aggregate popularity and usage of applications and extensions. If you are using an extension or application restricted to a certain audience, authentication tokens are sent with the update requests for these add-ons. For security reasons, Chrome also occasionally sends a cookieless request to the Chrome Web Store, in order to verify that installed extensions and applications that claim to be from the store are genuine.

In order to keep updates as small as possible, Google Chrome is internally split into a variety of components, each of which can be updated independently. Each component is uniquely identified via an ID that is shared among all Google Chrome installations (e.g., "fmeadaodfnidclnjhlkdjgkolmhmfofk"). An update request for a component contains this ID, the hash of the previous download (called a "fingerprint"), and the component's version. Because every installation has the same ID, and downloads of the same component have the same fingerprint, none of this information is personally identifiable.

If you install web apps on an Android device, a Google server is responsible for creating a native Android package that can be verified for authenticity by Chrome. When Chrome is updated or notices that the web app's manifest has changed, Chrome asks the server for a new version of the Android package in a cookieless request. If the information needed to create the native Android package cannot be acquired by the server (e.g., because the information is behind a corporate firewall), Chrome sends it to Google and an Android package is created that is unique to you. It contains a unique and random identifier that is not tied to your identity.

Chrome may also download and run a binary executable (e.g., as part of the software update or to improve Safe Browsing protection). These executables are cryptographically signed and verified before execution. Chrome may download further static resources like dictionaries on demand to reduce the size of the installer.

On Windows and OS X versions of Chrome, the recovery component tries to repair Google Update when it's broken. After the relevant binary is executed, Google Update uploads statistics on the actions that were performed. These statistics contain no personally identifiable information.

Network time

On desktop platforms, Chrome uses [network time](#) to verify SSL certificates, which are valid only for a specified time. At random intervals or when Chrome encounters an expired SSL certificate, Chrome may send requests to Google to obtain the time from a trusted source. These requests are more frequent if Chrome believes the system clock is inaccurate. These requests contain no cookies and are not logged on the server.

In order to measure the success rate of Google Chrome downloads and installations of the Windows version of Google Chrome, a randomly-generated token is included with Google Chrome's installer. This token is sent to Google during the installation process to confirm the success of that particular installation. A new token is generated for every install. It is not associated with any personal information, and is deleted once Google Chrome runs and checks for updates the first time.

For Chrome to know how many active installations it has, the mobile version of Chrome sends a ping to Google with a salted hash of a device identifier on an ongoing basis. The desktop version of Chrome does not send any stable identifier to count active installations. Instead an anonymous message to Google with a timestamp of the last ping is used to infer number of active installations.

Measuring effectiveness of a promotion

Chrome utilizes two measurements to understand how effective a promotional campaign has been: how many Chrome installations are acquired through a promotional campaign, and how much Chrome usage and traffic to Google is driven by a campaign.

To measure installations or reactivations of Chrome through a campaign, Chrome will send a token or an identifier unique to your device to Google at the first launch of Chrome, as well as the first search using Google. On desktop versions of Chrome, a token unique to your device is generated. The same token will be sent if Chrome is later reinstalled at first launch and at first use of the Omnibox after reinstallation or reactivation. Rather than storing the token on the computer, it is generated when necessary by using built-in system information that is scrambled in an irreversible manner. On iOS, Chrome uses the IDFA for counting installations acquired by a campaign, and it can be reset in iOS settings.

To measure searches and Chrome usage driven by a particular campaign, Chrome inserts a promotional tag, not unique to you or your device, in the searches you perform on Google. This non-unique tag contains information about how Chrome was obtained, the week when Chrome was installed, and the week when the first search was performed. For desktop versions of Chrome, Chrome generates a promotional tag, if the promotional installation token described in the previous paragraph indicates that Chrome has been installed or reactivated by a campaign on a device which has not been associated with any campaign yet. For Chrome on Mobile, a promotional tag is always sent regardless of the source of installations.

The promotional tag is generated using a software library called "RLZ" and looks similar to "1T4ADBR enUS236US239". The RLZ library was fully open-sourced in June 2010. For more information, please see the In the Open, for RLZ post on the Chromium blog and the article "How To Read An RLZ String". On Android, this promotional tag can also be a readable string like "android-hms-tmoble-us" instead of an RLZ string, and is not unique to either you or your device.

This non-unique promotional tag is included when performing searches via Google (the tag appears as a parameter beginning with "rlz=" when triggered from the Omnibox, or as an "x-rlz-string" HTTP header). We use this information to measure the searches and Chrome usage driven by a particular promotion.



If usage statistics and crash reports are enabled, the RLZ string is sent along with the report. This allows us to improve Chrome based on variations that are limited to specific geographic regions.

For the desktop version of Chrome, you can opt-out of sending this data to Google by uninstalling Chrome, and installing a version downloaded directly from www.google.com/chrome. To opt-out of sending the RLZ string in Chrome OS, press Ctrl + Alt + T to open the crash shell, type rlz disable followed by the enter key, and then reboot your device.

Usage statistics and crash reports

Chrome has a feature to automatically send usage statistics and crash reports to Google in order to help improve Chrome's feature set and stability.



Usage statistics contain information such as system information, preferences, user interface feature usage, responsiveness, and memory usage. This feature is enabled by default for Chrome installations of version 54 or later. You can enable or disable the feature in the "Privacy" section of Google Chrome's settings. These statistics do not include any personal information. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs or personal information depending on what was happening at the time of the crash.

When this feature is enabled, Google Chrome stores a randomly generated unique token on your device, which is sent to Google along with your usage statistics and crash reports. The token does not contain any personal information and is used to de-duplicate reports and maintain accuracy in statistics. This token is deleted when the feature is disabled and a new token is regenerated when the feature is enabled again.

Along with usage statistics and crash reports, Chrome also reports anonymous, randomized data that is constructed in a manner which is not linked to the unique token, and which ensures that no information can be inferred about any particular user's activity. This data collection mechanism is summarized on the Google research blog, and full technical

Chrome will also anonymously report to Google if requests to websites operated by Google fail or succeed in order to detect and fix problems quickly.

If you are also syncing your browsing history without a sync passphrase, Chrome usage statistics include information about the web pages you visit and your usage of them. The information will also include the URLs and statistics related to downloaded files. If you sync extensions, these statistics will also include information about the extensions that have been installed from Chrome Web Store. The URLs and statistics are sent along with a unique device identifier that can be reset by turning off history Sync or usage statistics and crash reports. The usage statistics are not tied to your Google account. Google only stores usage statistics associated with published extensions, and URLs that are known by Google's web crawlers. We use this information to improve our products and services, for example, by identifying web pages which load slowly; this gives us insight into how to best improve overall Chrome performance. We also make some statistics available externally, through efforts like the Chrome User Experience Report. Externally published reports are conducted in highly aggregated manner to not reveal individual user's identity.

On iOS, if you are syncing your browsing history without a sync passphrase, Chrome reports usage for certain URLs that other Google apps could open. For example, when you tap on an email address, Chrome presents a dialog that allows you to choose between opening with Google Gmail or other mail apps installed on your device. The usage information also includes which apps were presented to you, which one was selected, and if a Google app was installed. Chrome does not log the actual URL tapped. If you are signed in, this usage is tied to your Google account. If you are signed out, the information is sent to Google with a unique device identifier that can be regenerated by resetting the Google Usage ID found in Chrome settings. The raw reports are deleted within 60 days, after which only the aggregated statistics remain.

Google Surveys in Chrome

When you have "send usage statistics" enabled, you may be randomly selected to participate in surveys to evaluate consumer satisfaction with Chrome features. If you are selected, Chrome on Android requests a survey from Google for you. If a survey is available, Chrome then asks you to answer the survey and submit the responses to Google.

The survey also records basic metrics about your actions, such as time spent looking at the survey and elements that the user clicked. These metrics are sent to Google even if you do not fully complete the survey.

To ensure that surveys are spread evenly across users and not repeatedly served to a single user, the feature stores a randomly generated unique token on the device. This token is used solely for the survey requests and does not contain any personal information. If you disable sending usage statistics, the token will be cleared.

Suggestions for spelling errors

Desktop versions of Chrome can provide smarter spell-checking by sending text you type into the browser to Google's servers, allowing you to apply the same spell-checking technology that's used by Google products like Docs. If this feature is enabled, Chrome sends the entire contents of text fields as you type in them to Google, along with the browser's default language. Google returns a list of suggested spellings that are displayed in the context menu. Cookies are not sent along with these requests. Requests are logged temporarily and anonymously for debugging and quality improvement purposes.

This feature is disabled by default; to turn it on, click "Ask Google for suggestions" in the context menu that appears when you right-click on a misspelled word. You can also turn this feature on or off with the "Use a web service to help resolve spelling errors" checkbox in the Privacy section of Chrome settings. When the feature is turned off, spelling suggestions are generated locally without sending data to Google's servers.

Mobile versions of Chrome rely on the operating system to provide spell-checking.

Translate

Google Chrome's built-in translation feature helps you read more of the Web, regardless of the language of the web page. The feature is enabled by default.



Translation can be disabled at any time in Chrome's settings.

Language *detection* is done entirely using a client-side library, and does not involve any Google servers. For *translation*, the contents of a web page are only sent to Google if you explicitly decide to translate it by clicking "Translate" on the bar, or if you've previously chosen "Always translate" for a given language via the translate bar Options menu.

If you do choose to translate a web page, the text of that page is sent to Google Translate for translation. Your cookies are not sent along with that request and the request is sent over SSL. This communication with Google's translation service is covered by the Google privacy policy.

If you've chosen to sync your Chrome history, statistics about the languages of pages you visit and about your interactions with the translation feature will be sent to Google to improve Chrome's understanding of the languages you speak and when Chrome should offer to translate text for you.

Google Chrome provides the option to sign in with your Google Account and synchronize your Chrome data across multiple devices ("Sync"). Synced data can include bookmarks, saved passwords, open tabs, browsing history, extensions and more. In Advanced sync settings, you can choose which types of data to synchronize with this device. By default, all syncable data types are enabled.

On desktop versions of Chrome, signing into or out of any Google web service (e.g. google.com) also signs you into or out of Chrome. You can turn Sync on or off, or adjust which data is syncing, in the "People" section of Chrome settings. If you have turned on Sync and signed out of the account you are syncing to, Sync will pause sending all syncable data to Google until you sign back in with the same account. Some sync data types (such as bookmarks and passwords) that are saved locally while Sync is paused will automatically be synced to your account after you sign back in with the same account.

On mobile versions of Chrome, you can sign into or sign out of Chrome from Chrome settings. Signing into Chrome will also turn on Sync. This can be done for any account that has already been added to the mobile device without authenticating again.

On both desktop and mobile, signing into Chrome keeps you signed into Google web services until you sign out of Chrome. On mobile, signing into Chrome will keep you signed in with all Google Accounts that have been added to the device. On desktop, it will keep you signed in with all Google Accounts that you added from a Google web service, unless you have set "Keep local data only until you quit your browser" in your cookie settings.

On Android and desktop, Chrome signals to Google web services that you are signed into Chrome by attaching an X-Chrome-Connected and/or C-Chrome-ID-Consistency-Request header to any HTTPS requests to Google-owned domains. On iOS, the CHROME_CONNECTED cookie is used instead. This allows those Google web services to update their UI accordingly. If you are using a managed device, your system admin may disable the sign in feature or require that data be deleted when you disconnect your account.

Google uses your personal synchronized data to provide you a consistent browsing experience across your devices, and to customize features in Chrome. You can manage your synchronized history by going to chrome://history in your Chrome browser. If "Include history from Chrome and other apps in your Web & App Activity" is checked on the Web & App Activity controls page, Google also uses your synchronized browsing data to provide personalized Google products and services to you. You can change your preference any time, and manage individual activities associated with your Google account.

The paragraph above describes the use of your personal browsing history. Google also uses aggregated and anonymized synchronized browsing data to improve other Google products and services. For example, we use this information to improve Google Search by helping to detect mobile friendly pages, pages which have stopped serving content, and downloads of malware.

If you would like to use Google's cloud to store and sync your Chrome data without allowing any personalized and aggregated use by Google as described in the previous paragraphs, you can choose to encrypt all of your synced data with a sync passphrase. If you choose this option, it's important to note that Google won't have access to the sync passphrase you set; we won't be able to help you recover data if you forget the passphrase. Regardless of how you choose to encrypt your data, all data is always sent over secure SSL connections to Google's servers.

If you're signed into Chrome and are syncing passwords and/or other types of login credentials without a sync passphrase, these credentials are stored in your Google Account. Chrome may help you sign in with credentials you've saved in Android apps on websites that are associated with the respective apps. Likewise, credentials you've saved for websites can be used to help you sign into related Android apps. You can view the credentials you've saved in Chrome and Android by visiting passwords.google.com in any browser. If you've saved credentials for Android applications, Chrome periodically sends a cookieless request to Google to get an updated list of websites that are associated with those applications. To stop websites and Android apps from automatically signing in using credentials you previously saved, you can turn off Auto Sign-In on passwords.google.com or in Chrome settings under "Manage passwords". For more details see this article.

If you sync your browsing history without a Sync passphrase and your browser's usage statistics and crash reports setting is also enabled, your usage statistics and crash reports will include statistics about the pages you visit. You can read more in the Usage statistics and crash reports section of this Whitepaper.

All data synchronized through Google's servers is subject to Google's Privacy Policy. To get an overview of the Chrome data stored for your Google Account, go to the Chrome section of Google Dashboard. That page also allows you to stop synchronization completely and delete all sync data from Google's servers.

Autofill and Password Management

Google Chrome has a form autofill feature that helps you fill out forms on the web more quickly. Autofill is enabled by default, but it can be turned off at any time in Chrome's settings.

If Autofill is enabled and you encounter a web page containing a form, Chrome sends some information about that form to Google. This information includes a hash of the web page's hostname, as well as form identifiers (such as field names), the basic structure of the form, and Chrome's guess at each field's data type (for example, "field X looks like a phone number, and field Y looks like a country"). This information helps Chrome match up your locally stored Autofill data with the contents of the form, and it also helps to improve the quality of form-filling over time.

If Autofill is enabled when you submit a form, Chrome sends the data types you actually used in the form. This information helps Chrome improve its guesses over time. The actual text you typed into the form is not sent to Google.

You can manage your Autofill entries via [Chrome's settings](#), and you can edit or delete saved information at any time. Chrome will never store credit card information without explicit confirmation. If you scan your credit card using a phone camera, the recognition is performed locally.

Chrome may help you sign in to websites with credentials you've saved to Chrome's password manager or Google Smart Lock by autofilling sign-in forms, by offering you an account picker, or by automatically signing you in. You can manage and delete your saved credentials in the "Forms and passwords" section of Chrome's settings. If you enable [password management](#), the same kind of data about forms as described above is sent to Google to interpret password forms correctly and enable Chrome to offer password generation that meets site-specific requirements.

Also, if you choose, you can bring your Autofill data with you to all your Chrome-enabled devices by [syncing it](#) as part of your browser settings (see the "Sign In to Chrome" section of this document). If you choose to sync Autofill information, field values are sent as described in "Sign In to Chrome"; otherwise, field values are not sent.

Payments

If you are signed into Chrome and syncing credit cards and addresses with Google Pay, Chrome will offer to save your credit cards and related billing addresses to Google Pay and on your local device. Integration with Google Pay can be disabled via Chrome's Advanced sync settings. If integration with Google Pay is disabled, credit cards will be saved locally but will not be synced. If integration with Google Pay is enabled, Chrome may offer to autofill forms with credit card data stored in your Google Pay account. The cards from your Google Pay account not already saved locally are masked until you provide the correct CVV code. When providing your CVV code for verification, you can choose to store the credit card locally as part of your Chrome Autofill data. If you choose not to store the card locally, you will be prompted for your CVV code each time you use the card. If you use a card from Google Pay, Chrome will collect information about your computer and share it with Google Pay to prevent fraudulent use of your card.

To delete credit card information saved in Chrome, follow the "Add and edit credit cards" steps in [the Autofill article](#). When you delete a credit card that's also saved in your Google Pay account, you will be redirected to the Google Pay to complete the deletion. After your card has been deleted from your Google Pay account, Chrome will automatically remove that card from your Autofill suggestions.

Chrome also supports the [PaymentRequest API](#) by allowing you to pay for purchases with credit cards from Autofill, Google Pay, and other payment apps already installed on your device. Google Pay and other payment apps are only available on an Android device. PaymentRequest allows the merchant to request the following information: full name, shipping address, billing address, phone number, email, credit card number, credit card expiration, CVV, and Google Pay credentials. Information is not shared with the merchant until you agree.

Geolocation

Google Chrome supports the [Geolocation API](#), which provides access to fine-grained user location information with your consent.

By default, Chrome will request your permission when a web page asks for your location information, and does not send any location information to the web page unless you explicitly consent.

Furthermore, whenever you are on a web page which is using your location information, Chrome will display a location icon on the right side of the omnibox. You can click on this icon in order to find out more information or manage location settings.



In [Chrome's settings](#), by clicking "Show advanced settings.", then clicking "Content Settings" and scrolling to the "Location" section, you can choose to allow all sites to receive your location information, have Chrome ask you every time (the default), or block all sites from receiving your location information. You can also configure exceptions for specific web sites.

In the Android version of Chrome, your default search engine automatically receives your location when you conduct a search. On the iOS version of Chrome, by default your location is sent to Google if you conduct a search from the omnibox. Read more about how your default search engine handles geolocation and how to manage your settings in the [Omnibox](#) section of the whitepaper.

If you do choose to share your location with a web site, Chrome will send local network information to Google (also used by other browsers such as Mozilla Firefox) in order to estimate your location. This local network information can include data about nearby Wi-Fi access points or cellular signal sites/towers (even if you're not using them), and your computer's IP address. The requests are logged, and aggregated and anonymized before being used to operate, support, and improve the overall quality of Google Chrome and Google Location Services.

For further reading on the privacy and user interface implications of the Geolocation API (as well as other HTML5 APIs), see ["Practical Privacy Concerns in a Real World Browser"](#) written by two Google Chrome team members.

Speech to text

Chrome supports the Web Speech API, a mechanism for converting speech to text on a web page. It uses Google's servers to perform the conversion. Using the feature sends an audio recording to Google (audio data is not sent directly to the page itself), along with the domain of the website using the API, your default browser language and the language settings of the website. Cookies are not sent along with these requests.

Google Assistant "Ok Google"

The Google Assistant feature is integrated into some models of Chrome OS devices. If you opt in to the feature, Chrome OS listens for you to say "Ok Google" and sends the audio of the next thing you say, plus a few seconds before, to Google. Detection of the phrase "Ok Google" is performed locally on your computer, and the audio is only sent to Google after it detects "Ok Google". You can enable or disable this feature in Google Assistant Settings.

Enabling this feature in Chrome Settings will cause Chrome to listen whenever the screen is unlocked. On Chrome OS devices with a local audio processor, the device also listens when the device is asleep. On these devices, The Google Assistant feature only works if Voice & Audio Activity is enabled for your Google account. Chrome will prompt you to enable Voice & Audio Activity for the associated Google account if it is disabled.

Once the audio has been converted to text, a search with that text is submitted to Google. If you have used the "Ok Google" search before on a device but turned off Voice & Audio Activity later, your device is still capable of processing your voice and sending the audio to Google but the voice is deleted shortly.

You can determine your Chrome OS device's behavior by examining the text in the "Search and Assistant" section of settings.

Google Cloud Print

The Google Cloud Print feature allows you to print documents from your browser over the Internet. You do not need a direct connection between the machine that executes Chrome and your printer.

If you choose to print a web page via Cloud Print, Chrome will generate a PDF of this website and upload it over an encrypted network connection to Google's servers. If you choose to print other kinds of documents, they may be uploaded as raw documents to Google's servers.

A print job will be downloaded by either a Chrome browser ("Connector") or a Cloud Print capable printer that you selected when printing the website. In some cases the print job must be submitted to a third-party service to print (HP's ePrint, for example).

The print job is deleted from Google's servers when any of three criteria is met:

- You delete the print job
- The job has been printed and marked as printed by the printer/connector
- The job has been queued on Google's servers for 30 days

You can manage your printers and print jobs on the Google Cloud Print website.

SSL certificate reporting

Chrome stores locally a list of expected SSL certificate information for a variety of high-value websites, in an effort to prevent man-in-the-middle attacks. For Google websites and other websites that choose to opt in, Chrome will report a possible attack or misconfiguration. If the certificate provided by the web server doesn't match the expected signature, Chrome reports information about the SSL certificate chain to Google or to a report collection endpoint of the website's choosing. Chrome sends these reports only for certificate chains that use a public root of trust.

Chrome also allows users to choose to send information that helps Google improve SSL warnings and error pages. You can opt in to this feature by checking the box on any SSL error page. While you are opted in, each time you see an SSL error page, a report will be sent to Google's security team. The report contains the SSL certificate chain, the server's hostname, the local time, and relevant details about the validation error and SSL error page type. Because Chrome sends these reports for all certificate chains, even those that chain to a private root of trust, these chains can contain personally identifiable information. You can opt out anytime by unchecking the box "Automatically report details of possible security incidents to Google" in the Privacy section of Chrome's advanced settings.

The SSL certificate reporting feature is not available on Chrome iOS.

Token Binding

Chrome's Token Binding feature allows a server to validate in a strong way that new HTTPS sessions originate from the same client as a previous session. This assertion mitigates the risk of session theft because cookies can be cryptographically tied to a particular Token Binding ID. This feature makes it significantly more difficult to convert stolen cookies into stolen sessions. On the iOS version of Chrome, Token Binding is not used for requests made for web page loading.

Token Binding IDs do not contain any information about the user, and a different Token Binding ID is created for each secure origin. A Token Binding ID created for one server will be shared with another server only if the original server requests it to be shared. Token Binding IDs are not shared between Chrome profiles, and all Token Binding IDs created during Incognito browsing are destroyed when you exit the Incognito session. Note that Token Bindings are not used for requests that block cookies.

On desktop versions of Chrome, you can determine which Token Binding IDs have been created (and you can remove unwanted IDs) in the Cookies and Site Data dialog (available at <chrome://settings/siteData>). On all platforms, Token Binding IDs are subject to removal when "Cookies and Site Data" are cleared via the "Clear Browsing Data" dialog (<chrome://settings/clearBrowserData>). Token Binding is an evolution of the TLS Channel ID feature.

For more technical details and background information, visit browserauth.net and the work-in-progress [IETF draft](#).

Installed Applications and Extensions

Users can install external apps and extensions for the desktop versions of Chrome to add features to or customize their Chrome browsers. Installing an application or extension from the Chrome Web Store directly or via an [inline installation](#) flow on a third-party site involves a request to the Chrome Web Store for details about the application. This request includes cookies, and if you're logged into Google when you install an application, that installation is recorded as part of your Google account. The store uses this information to recommend applications to you in the future, and in aggregate to evaluate application popularity and usage. As noted above, applications and extensions are updated via Google Update.

As they're more deeply integrated into Chrome, applications and extensions that you choose to install can request access to additional capabilities, enabling functionality that doesn't make sense on the web at large: background notifications or raw socket access, for instance. These additional permissions may change the way your data is collected and shared, as extensions and applications might have access to data regarding the websites you visit, and might be capable of monitoring or modifying your interactions with the web. When installing an application or extension, Chrome may first warn you about [certain capabilities](#). Please do take the time to read and evaluate this warning before proceeding with the installation. Note also that interactions with and data collected by these third-party applications and extensions are governed by their own privacy policies, not Google's privacy policy.

Push messaging

Your device may receive push messages from the backend servers of apps and extensions installed in Chrome, websites that you grant the "notification" permission to, and your default search engine. Disabling push messages from your default search engine is done in the same way as disabling push messages from any site, by visiting the "Notifications" section of "Site settings".

Push message data is sent over a secure channel from the developer through Google's infrastructure to Chrome on your device, which can wake up apps, extensions, and websites (including your default search engine) to deliver the message. The developer may end-to-end encrypt the message data, or may send it in a form such that Google servers process it as plain text. Google servers retain up to 4 weeks' worth of messages to ensure delivery to users even if their devices are offline at the time of the initial pushing.

If the notification permission is set to "granted" for any website (including the default search engine), or you have an app or extension installed that uses push messaging, then Chrome provides the app's, extension's, or website's server with one or more registration tokens that can be used to send messages to the entity (app, extension, or website). Websites you visit in Incognito mode are not allowed to send you push messages and therefore cannot get a registration token.

When you uninstall an app or extension, revoke the notification permission for a website, or clear cookies for a permitted website, its registration token is revoked and will not be reused, even if the same app or extension is re-installed or the same website is re-visited. Registration tokens used by Chrome components such as [Sync](#) are revoked once they are no longer in use (for example, when the user disables Sync). When a registration token is revoked, the associated entity on your device stops receiving messages sent from its developer's server.

The registration tokens that are passed to entities contain an encrypted device ID, which is used for routing the messages. Google can decrypt the device ID, but other entities cannot, and the encryption is designed so that two registration tokens for the same device ID cannot be correlated. On desktop versions of Chrome, the device ID is reset when the Chrome profile is removed (via the "People" section in Chrome's Settings), or when neither Chrome Sync nor any of the entities requires it for push messaging. On Android, the lifetime of the device ID is governed by the operating system and is independent of Chrome. Any messages routed to registration tokens containing a revoked device ID will not be delivered.

Chrome custom tabs

On Android devices, an app developer may use a Custom Tab to show web content when you click on a URL from their app. A Custom Tab may look different from a regular Chrome tab, for example it may have app-specified visual style, and the absence of an editable URL bar. Despite the different visual style a Custom Tab may have, the data sent and received in the Custom Tab, such as cookies, saved passwords and browsing history function the same way they do in a normal Chrome tab. The Custom Tab is an app-customized view using the same underlying user profile.

With Chrome Custom Tabs, an Android app developer may also specify custom actions in the Chrome toolbar and overflow menu that are relevant to their app, for example, "share", "save page", "copy URL". If you tap on such a button, the address of the current website is shared with the application.

An application can request Chrome to pre-render a given URL in the background. This allows Chrome to show you a pre-loaded site instantly when you open it from the app. At the same time it allows an application to set cookies in your browser in the background. To disable pre-rendering, you can uncheck "Prefetch page resources" in the privacy settings.

If you have selected the option to “Continue where you left off” in settings on desktop versions of Chrome, when you open Chrome, it attempts to bring you right back to the way things were when the browser was closed. Chrome reloads the tabs you had open and persists session information to get you up and running as quickly as possible. This feature effectively extends a browsing session across restarts. In this mode, session cookies are no longer deleted when the browser closes; instead, they remain available on restart to keep you logged into your favorite sites.

On desktop versions of Chrome, this feature can be enabled or disabled in Chrome settings. On Chrome OS, it is enabled by default.

On OS X, when you restart your device, a checkbox in the OS confirmation dialog asks you whether you want to re-open applications and windows after restart. If you check this box, Chrome restores tabs and windows, as well as the session cookies, even if you have disabled “Continue where you left off” on Chrome.

On mobile versions of Chrome, this feature is always enabled without a setting.

Chrome Variations

We want to build features that users want, so a subset of users may get a sneak peek at new functionality being tested before it’s launched to the world at large. A list of field trials that are currently active on your installation of Chrome will be included in all requests sent to Google. This Chrome-Variations header (X-Client-Data) will not contain any personally identifiable information, and will only describe the state of the installation of Chrome itself, including active variations, as well as server-side experiments that may affect the installation.

The variations active for a given installation are determined by a seed number which is randomly selected on first run. If usage statistics and crash reports are disabled, this number is chosen between 0 and 7999 (13 bits of entropy). If you would like to reset your variations seed, run Chrome with the command line flag “--reset-variation-state”. Experiments may be further limited by country (determined by your IP address), operating system, Chrome version and other parameters.

Do Not Track

If you enable the “Do Not Track” preference in Chrome’s settings, Chrome will send a DNT:1 HTTP header with your outgoing HTTP, HTTPS and SPDY browsing traffic (Chrome cannot, however, guarantee that NPAPI plugins also send the header.) The header will not be sent with system traffic such as the geolocation, metrics or device management services.

The effect of Do Not Track depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example, to improve security; to provide content, services, ads and recommendations on their websites; and to generate reporting statistics.

Chrome on iOS now uses WKWebView to provide a more stable and faster browser. As a result of this move, the Do Not Track preference is no longer available due to iOS constraints. If Apple makes changes to allow this feature, Chrome will make Do Not Track available again in iOS.

Plugins

Chrome ships with an Adobe Flash Player implementation that is based on the Pepper API. Flash and other Pepper-based plugins may ask you for “Access to your computer”. If you grant this permission, the plugin is granted unsandboxed access. This allows content providers to offer you access to DRM protected content like videos or music but may have security and privacy implications, so consider carefully whether you trust a plugin or website with this privilege.

Media licenses

Some websites encrypt media to protect against unauthorized access and copying. When users play media from these sites, they typically log into the site, which authenticates the user, and then digital rights management negotiates a key exchange for the decryption and playback of the media.

For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. The implementation of that API is tightly coupled with the browser to protect user privacy and security, through Content Decryption Modules (CDM), which are provided by digital rights management solutions such as Google Widevine or Microsoft PlayReady.

When a user asks Chrome to play encrypted HTML5 media (for example, watching a movie on Google Play Movies), Chrome will generate a request for a license to decrypt that media. This license request contains an automatically generated request ID, which is created by the Content Decryption Module, as well as proof that the CDM is legitimate. After generation, the license request is typically sent to a license server managed by either the content website or Google. Neither the license request, the proof, nor the request ID include any personally identifying information. After being sent, the license request is not stored locally on the user’s device.

As part of the license request, Chrome also generates a unique session ID which does not contain personally identifying information. This session ID is sent to the license server, and when the server returns a license the session ID is used to decrypt the media. The session ID may be stored locally even after the site has been closed. The license may also be

When returning a license, the site license server may include a client ID, generated by the site. This client ID is unique to the user and the site, it is not shared between sites. If provided, the client ID is stored locally and included by Chrome in subsequent license requests to that site. The client ID may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Media licenses” enabled.

On some platforms, the website may additionally request verification that the device is eligible to play specific types of protected content; on Chrome OS, this is known as [Verified Access](#)). In this case, Google creates a certificate using a unique hardware identifier for the device. This hardware ID identifies the device, but does not identify the user. If the user agrees, Google receives the hardware ID and generates a certificate verifying the device for the requested site. The certificate does not include the hardware ID or any other information that could permanently identify the device. Certificates are stored locally similar to other cached browsing data, and may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Media licenses” enabled.

Some sites use Flash instead of HTML5. If a website you visit chooses to use Adobe Flash Access DRM protection, Chrome for Windows and Chrome OS will give Adobe Flash access to a device identifier. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with “Media licenses” enabled.

In order to give you access to licensed music, the [Google Play Music app](#) can retrieve a device identifier that is derived from your hard drive partitions or, on a Chrome OS or Linux installation, from a unique file on your disk. This identifier can be reset by reinstalling your operating system.

Cloud policy

When you sign into a Chrome OS device, Chrome on Android, or a desktop Chrome profile with an account associated with a Google Apps domain, Chrome checks whether the domain has configured enterprise policies. If so, the Chrome OS user session or Chrome profile is assigned a unique ID, and registered as belonging to that domain. Any configured policies are applied to the profile. In order to revoke the registration, you'll need to remove the Chrome OS user profile, sign out of Chrome on Android, or remove the desktop profile.

Additionally, Chrome OS devices can be enrolled to a Google Apps domain by a domain admin. This will enforce enterprise policies for the entire device, such as providing shared network configurations and restricting access to developer mode. When a Chrome OS device is enrolled to a domain, then a unique device ID is registered to the device. In order to revoke the registration, the admin will need to wipe the entire Chrome OS device.

Registered profiles and devices check for policy changes periodically (every 3 hours by default). In some cases, the server pushes policy changes to the client without waiting for Chrome's periodic check. Unregistered profiles check whether a policy has been turned on for their domain each time Chrome starts up.

The [policy list](#) contains details about the types of configurations that are available via Cloud Policy.

Data Saver

If you enable Data Saver, Chrome will send your HTTP traffic through Google's optimizing proxy servers. This option reduces the amount of data downloaded, and protects you against malware and phishing via the [Safe Browsing](#) service. You can find more information about the data compression benefits on the [Chromium blog](#).

The proxy service is disabled for connections to HTTPS origins and connections made from Incognito tabs. These connections are not routed through Google's servers. For connections to HTTP origins, request URLs are logged. Cookies and If-None-Match headers are stripped from the logs. Additionally, the content of proxied pages is also cached but not logged. The logs are not associated with your Google Account, and the entire log entry is removed within 6 months. These logs are also governed by standard Google search logging policies.

Google uses the logged and cached data to improve both Data Saver and Safe Browsing; for example, more effective optimizations can be uncovered by analyzing timing data for pages loaded through the proxy service, and malware can be detected more rapidly by analyzing response data in realtime.

Your IP address is forwarded to the origin HTTP server via an X-Forwarded-For header, in accordance with the HTTP standard. The Data Saver service is a transparent proxy, *not* an anonymization service.

By default, the connection between the browser and the Data Saver proxy is over an encrypted channel. However, a network administrator can [disable](#) the use of an encrypted channel to Data Saver.

Supervised Users

If you create a supervised user on Chrome or Chrome OS, certain information such as the supervised user's browsing activity, profile settings and permissions requests for blocked content will be sent to Google in association with your Google Account. You can access the browsing activity of your supervised users at [chrome.com/manage](#). In order to remove data that is associated with a supervised user from Google's servers, please sign in to your Google Account at [chrome.com/manage](#) and delete the respective supervised user.

Using Chrome with a kid's Google Account

Chrome for Android offers features to be used when signed in with a kid's Google Account and automatically signs in a kid's account if they've signed into the Android device. Chrome uses the [Sync](#) feature to sync settings configured by parents to the kid's account. You can read about how Sync data is used in the [Sign in](#) section of this Whitepaper.

The collection and use of Chrome data in association with a kid's Google Account are governed by the [Google Family Link - Children's Privacy Policy](#).

In order for the configured settings to apply to a kid's account, Chrome does not support the following features for a kid's Google Account: signing out of Chrome, [Incognito mode](#), and deleting browsing history from within Chrome. Browsing history can still be removed in the [Chrome section of the Google Dashboard](#).

By default, first party cookie blocking is disabled when Chrome is signed in with a kid's account. Parents can go to [chrome.google.com/manage/family](#) to allow their kids to block first party cookies. However, blocking cookies signs kids out of Google web products such as Google Search or YouTube and therefore prevents these products from providing any features designed for kids' Google Accounts.

When Chrome is used with a kid's Google Account, information about the kid's requests to access blocked content is sent to Google and made visible to the kid's parent(s) on [chrome.google.com/manage/family](#) and in the [Google Family Link app](#). If the kid's browsing mode is set to "Try to block mature sites", Chrome will send a request to the Google [SafeSearch service](#) for each navigation in order to block access to sites that have been classified as containing mature content.

Incognito and Guest Mode

Incognito mode in Chrome is a temporary browsing mode. It ensures that you don't leave browsing history and cookies on your computer. The browsing history and cookies are deleted only once you have closed the last incognito window. Incognito mode cannot make you invisible on the internet. Websites that you navigate to may record your visits. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Browsing as a Guest in Chrome allows you to use somebody else's computer without modifying their profile. For example, no bookmarks or passwords get stored on their computer. Note that Guest mode does not protect you for example, if the computer you are using is infected by a keylogger that records what you type.

iOS 8 and Mac OS X Yosemite Handoff Support

While browsing in a standard (i.e. non-Incognito) session, Chrome will share your current URL with iOS 8+ to support the Handoff feature that was added in OS X Yosemite. This information is only sent to Apple devices that are paired with your iOS device, and the data is encrypted in transit.

More information is available at [Apple Support](#), [Apple Developers](#), and in the [Apple iOS Security Guide](#). Chrome support for this feature can be disabled in Chrome settings.

Security Key

A FIDO U2F Security Key provides a non-phishable credential which can be used to authenticate a user. This mitigates the risk of various kinds of man-in-the-middle attacks in which websites try to steal your password and use it later.

To prevent abuse, a website is required to be delivered over a secure connection (HTTPS), and to register the security key before it can be used for identification. Once a website is registered with a specific security key, that security key will provide a persistent identifier, regardless of which computer it is plugged into, or whether you're in incognito or guest mode, but you must physically interact with the security key to give a website access to an identifier (by, for example, touching it, or plugging it in).

Physical Web

The Physical Web lets you see a list of URLs being broadcast by objects in the environment around you. Google Chrome looks for Physical Web devices with Bluetooth Low Energy beacons that are broadcasting URLs using the Eddystone protocol. Bluetooth signals can be received from 90 feet away or more, depending on signal strength and the user's environment (although the range is often much shorter, due to obstacles and signal noise). If the Physical Web feature is enabled, Chrome sends detected URLs to Google's Physical Web Service (PWS) via a cookieless HTTPS request. For each URL, the PWS obtains the title of the web page, filters out unsafe results, and returns a ranking based on non-personalized signals about the quality and relevance of the web page.

The Physical Web feature is available on Chrome on iOS and Android. Users will need to turn on Bluetooth to use the feature.

If Android users have location settings enabled on both their device and in Chrome, they will receive a notification the first time they are near a beacon that will give them the option to turn on the Physical Web feature. This beacon's URL is not sent to Google's PWS unless the Physical Web feature is enabled. Users can also [enable](#) (or disable) the feature in the Privacy settings. Once a user enables the feature, Chrome scans for nearby devices for a few seconds each time the user unlocks the mobile device in use and sends them to the PWS in order to obtain more information about the beacon. The user receives a silent notification when Chrome finds a nearby URL.

On iOS devices, users can [enable](#) (or disable) the feature in the Privacy settings or by adding the [Chrome widget to their Today view](#) in the notification center. Additionally, the feature is automatically enabled for users who have

location enabled on their device, granted Chrome the location permission, and have granted Google the geolocation permission. Chrome scans for nearby devices whenever it is open in the foreground. When Chrome finds nearby URLs, users will see them as omnibox suggestions. Additionally, Chrome scans for nearby devices for a few seconds when the Today widget is displayed in the notification center.

Bluetooth

Google Chrome supports the Web Bluetooth API, which provides websites with access to nearby Bluetooth Low Energy devices with your consent.

Chrome does not let any page communicate with a device unless you explicitly consent. When a web page asks to pair with a device, Chrome will ask you to choose which device the web page should access, if any. Selecting a device for one page does not give other pages access to the device you have chosen, and does not allow that page to access other devices. Currently, permission for a page to communicate with a device is usually revoked when the page is reloaded, and is always revoked when Chrome is restarted.

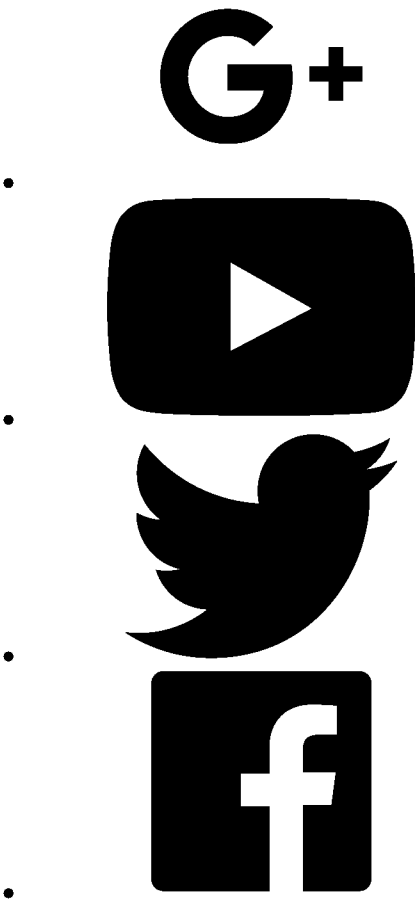
Chrome data that Android sends to Google

The data collection and usage described in this section is handled by Android and governed by the Google Privacy Policy.

If the Android Backup Service is enabled on your device, some of your Chrome preferences will be saved and stored on Google servers. For Nexus and Android One devices, it is described under “Back up your data and settings with Android Backup Service” in this article. For other Android devices, you may be able to find help by looking up your device on this page. When setting up a new Android device, you may request that it copies the preferences from a previously set up device. If you do so, Android may restore backed up Chrome preferences when Chrome is first installed. The new device only copies the preferences if automatic restore is enabled (see “Restore your data and settings” in the same article), Chrome was signed into an account when the backup was made, and the new Android device is signed into that same account.

Chrome’s backup data for a particular device may also be restored if you uninstall and then later re-install Chrome on that device. This will only happen if automatic restore is enabled and the device is signed into the account that Chrome was signed into when the backup was made.

Follow us





Chrome Family

- [Other Platforms](#)
- [Chromebooks](#)
- [Chromecast](#)
- [Chrome Cleanup Tool](#)



Enterprise

- [Google Chrome Browser](#)
- [Devices](#)
- [Google Cloud](#)
- [G Suite](#)



Education

- [Google Chrome Browser](#)
- [Devices](#)
- [Web Store](#)



Dev and Partners

- [Chromium](#)
- [Chrome OS](#)
- [Chrome Web Store](#)
- [Chrome Experiments](#)
- [Chrome Beta](#)
- [Chrome Dev](#)
- [Chrome Canary](#)



Stay Connected

- [Google Chrome Blog](#)
- [Chrome Help](#)



- [Privacy and Terms](#)
- [About Google](#)
- [Google Products](#)



[Help](#)

[Close](#)

Download Chrome for Windows

For Windows 10/8.1/8/7 32-bit.

For Windows 10/8.1/8/7 64-bit.

This computer will no longer receive Google Chrome updates because Windows XP and Windows Vista are no longer supported.

Download Chrome for Mac

For Mac OS X 10.10 or later.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

Download Chrome for Linux

Debian/Ubuntu/Fedora/openSUSE.

Please select your download package:

- ☒ 64 bit .deb (For Debian/Ubuntu)
☐ 64 bit .rpm (For Fedora/openSUSE)

Not Debian/Ubuntu or Fedora/openSUSE? There may be a community-supported version for your distribution [here](#).

Download Chrome for iOS

Google Chrome Terms of Service

These Terms of Service apply to the executable code version of Google Chrome. Source code for Google Chrome is available free of charge under open source software license agreements at <https://code.google.com/chromium/terms.html>.

1. Your relationship with Google

1.1 Your use of Google's products, software, services and web sites (referred to collectively as the "Services" in this document and excluding any services provided to you by Google under a separate written agreement) is subject to the terms of a legal agreement between you and Google. "Google" means Google Inc., whose principal place of business is at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States. This document explains how the agreement is made up, and sets out some of the terms of that agreement.

1.2 Unless otherwise agreed in writing with Google, your agreement with Google will always include, at a minimum, the terms and conditions set out in this document. These are referred to below as the "Universal Terms". Open source software licenses for Google Chrome source code constitute separate written agreements. To the limited extent that the open source software licenses expressly supersede these Universal Terms, the open source licenses govern your

1.3 Your agreement with Google will also include the terms set forth below in the Google Chrome Additional Terms of Service and terms of any Legal Notices applicable to the Services, in addition to the Universal Terms. All of these are referred to below as the “Additional Terms”. Where Additional Terms apply to a Service, these will be accessible for you to read either within, or through your use of, that Service.

1.4 The Universal Terms, together with the Additional Terms, form a legally binding agreement between you and Google in relation to your use of the Services. It is important that you take the time to read them carefully. Collectively, this legal agreement is referred to below as the “Terms”.

1.5 If there is any contradiction between what the Additional Terms say and what the Universal Terms say, then the Additional Terms shall take precedence in relation to that Service.

2. Accepting the Terms

2.1 In order to use the Services, you must first agree to the Terms. You may not use the Services if you do not accept the Terms.

2.2 You can accept the Terms by:

(A) clicking to accept or agree to the Terms, where this option is made available to you by Google in the user interface for any Service; or

(B) by actually using the Services. In this case, you understand and agree that Google will treat your use of the Services as acceptance of the Terms from that point onwards.

3. Language of the Terms

3.1 Where Google has provided you with a translation of the English language version of the Terms, then you agree that the translation is provided for your convenience only and that the English language versions of the Terms will govern your relationship with Google.

3.2 If there is any contradiction between what the English language version of the Terms says and what a translation says, then the English language version shall take precedence.

4. Provision of the Services by Google

4.1 Google has subsidiaries and affiliated legal entities around the world (“Subsidiaries and Affiliates”). Sometimes, these companies will be providing the Services to you on behalf of Google itself. You acknowledge and agree that Subsidiaries and Affiliates will be entitled to provide the Services to you.

4.2 Google is constantly innovating in order to provide the best possible experience for its users. You acknowledge and agree that the form and nature of the Services which Google provides may change from time to time without prior notice to you.

4.3 As part of this continuing innovation, you acknowledge and agree that Google may stop (permanently or temporarily) providing the Services (or any features within the Services) to you or to users generally at Google’s sole discretion, without prior notice to you. You may stop using the Services at any time. You do not need to specifically inform Google when you stop using the Services.

4.4 You acknowledge and agree that if Google disables access to your account, you may be prevented from accessing the Services, your account details or any files or other content which is contained in your account.

5. Use of the Services by you

5.1 You agree to use the Services only for purposes that are permitted by (a) the Terms and (b) any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries).

5.2 You agree that you will not engage in any activity that interferes with or disrupts the Services (or the servers and networks which are connected to the Services).

5.3 Unless you have been specifically permitted to do so in a separate agreement with Google, you agree that you will not reproduce, duplicate, copy, sell, trade or resell the Services for any purpose.

5.4 You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) any breach of your obligations under the Terms and for the consequences (including any loss or damage which Google may suffer) of any such breach.

6. Privacy and your personal information

6.1 For information about Google’s data protection practices, please read Google’s privacy policy at <https://www.google.com/privacy.html> and at <https://www.google.com/intl/en/chrome/privacy/>. This policy explains how Google treats your personal information, and protects your privacy, when you use the Services.

6.2 You agree to the use of your data in accordance with Google’s privacy policies.

7.1 You understand that all information (such as data files, written text, computer software, music, audio files or other sounds, photographs, videos or other images) which you may have access to as part of, or through your use of, the Services are the sole responsibility of the person from which such content originated. All such information is referred to below as the "Content."

7.2 You should be aware that Content presented to you as part of the Services, including but not limited to advertisements in the Services and sponsored Content within the Services may be protected by intellectual property rights which are owned by the sponsors or advertisers who provide that Content to Google (or by other persons or companies on their behalf). You may not modify, rent, lease, loan, sell, distribute or create derivative works based on this Content (either in whole or in part) unless you have been specifically told that you may do so by Google or by the owners of that Content, in a separate agreement.

7.3 Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some of the Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings (see <https://support.google.com/websearch/answer/510?hl=en>). In addition, there are commercially available services and software to limit access to material that you may find objectionable.

7.4 You understand that by using the Services you may be exposed to Content that you may find offensive, indecent or objectionable and that, in this respect, you use the Services at your own risk.

7.5 You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) any Content that you create, transmit or display while using the Services and for the consequences of your actions (including any loss or damage which Google may suffer) by doing so.

8. Proprietary rights

8.1 You acknowledge and agree that Google (or Google's licensors) own all legal right, title and interest in and to the Services, including any intellectual property rights which subsist in the Services (whether those rights happen to be registered or not, and wherever in the world those rights may exist).

8.2 Unless you have agreed otherwise in writing with Google, nothing in the Terms gives you a right to use any of Google's trade names, trade marks, service marks, logos, domain names, and other distinctive brand features.

8.3 If you have been given an explicit right to use any of these brand features in a separate written agreement with Google, then you agree that your use of such features shall be in compliance with that agreement, any applicable provisions of the Terms, and Google's brand feature use guidelines as updated from time to time. These guidelines can be viewed online at <https://www.google.com/permissions/guidelines.html> (or such other URL as Google may provide for this purpose from time to time).

8.4 Google acknowledges and agrees that it obtains no right, title or interest from you (or your licensors) under these Terms in or to any Content that you submit, post, transmit or display on, or through, the Services, including any intellectual property rights which subsist in that Content (whether those rights happen to be registered or not, and wherever in the world those rights may exist). Unless you have agreed otherwise in writing with Google, you agree that you are responsible for protecting and enforcing those rights and that Google has no obligation to do so on your behalf.

8.5 You agree that you shall not remove, obscure, or alter any proprietary rights notices (including copyright and trade mark notices) which may be affixed to or contained within the Services.

8.6 Unless you have been expressly authorized to do so in writing by Google, you agree that in using the Services, you will not use any trade mark, service mark, trade name, logo of any company or organization in a way that is likely or intended to cause confusion about the owner or authorized user of such marks, names or logos.

9. License from Google

9.1 Google gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by Google as part of the Services as provided to you by Google (referred to as the "Software" below). This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Google, in the manner permitted by the Terms.

9.2 Subject to section 1.2, you may not (and you may not permit anyone else to) copy, modify, create a derivative work of, reverse engineer, decompile or otherwise attempt to extract the source code of the Software or any part thereof, unless this is expressly permitted or required by law, or unless you have been specifically told that you may do so by Google, in writing.

9.3 Subject to section 1.2, unless Google has given you specific written permission to do so, you may not assign (or grant a sub-license of) your rights to use the Software, grant a security interest in or over your rights to use the Software, or otherwise transfer any part of your rights to use the Software.

10. Content license from you

10.1 You retain copyright and any other rights you already hold in Content which you submit, post or display on or through, the Services.

11. Software updates

11.1 The Software which you use may automatically download and install updates from time to time from Google. These updates are designed to improve, enhance and further develop the Services and may take the form of bug fixes, enhanced functions, new software modules and completely new versions. You agree to receive such updates (and permit Google to deliver these to you) as part of your use of the Services.

12. Ending your relationship with Google

12.1 The Terms will continue to apply until terminated by either you or Google as set out below.

12.2 Google may at any time, terminate its legal agreement with you if:

- (A) you have breached any provision of the Terms (or have acted in manner which clearly shows that you do not intend to, or are unable to comply with the provisions of the Terms); or
- (B) Google is required to do so by law (for example, where the provision of the Services to you is, or becomes, unlawful); or
- (C) the partner with whom Google offered the Services to you has terminated its relationship with Google or ceased to offer the Services to you; or
- (D) Google is transitioning to no longer providing the Services to users in the country in which you are resident or from which you use the service; or
- (E) the provision of the Services to you by Google is, in Google's opinion, no longer commercially viable.

12.3 Nothing in this Section shall affect Google's rights regarding provision of Services under Section 4 of the Terms.

12.4 When these Terms come to an end, all of the legal rights, obligations and liabilities that you and Google have benefited from, been subject to (or which have accrued over time whilst the Terms have been in force) or which are expressed to continue indefinitely, shall be unaffected by this cessation, and the provisions of paragraph 19.7 shall continue to apply to such rights, obligations and liabilities indefinitely.

13. EXCLUSION OF WARRANTIES

13.1 NOTHING IN THESE TERMS, INCLUDING SECTIONS 13 AND 14, SHALL EXCLUDE OR LIMIT GOOGLE'S WARRANTY OR LIABILITY FOR LOSSES WHICH MAY NOT BE LAWFULLY EXCLUDED OR LIMITED BY APPLICABLE LAW. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR CONDITIONS OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR LOSS OR DAMAGE CAUSED BY NEGLIGENCE, BREACH OF CONTRACT OR BREACH OF IMPLIED TERMS, OR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, ONLY THE LIMITATIONS WHICH ARE LAWFUL IN YOUR JURISDICTION WILL APPLY TO YOU AND OUR LIABILITY WILL BE LIMITED TO THE MAXIMUM EXTENT PERMITTED BY LAW.

13.2 YOU EXPRESSLY UNDERSTAND AND AGREE THAT YOUR USE OF THE SERVICES IS AT YOUR SOLE RISK AND THAT THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE."

13.3 IN PARTICULAR, GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO YOU THAT:

- (A) YOUR USE OF THE SERVICES WILL MEET YOUR REQUIREMENTS,
- (B) YOUR USE OF THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR,
- (C) ANY INFORMATION OBTAINED BY YOU AS A RESULT OF YOUR USE OF THE SERVICES WILL BE ACCURATE OR RELIABLE, AND
- (D) THAT DEFECTS IN THE OPERATION OR FUNCTIONALITY OF ANY SOFTWARE PROVIDED TO YOU AS PART OF THE SERVICES WILL BE CORRECTED.

13.4 ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICES IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR OTHER DEVICE OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL.

13.5 NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM GOOGLE OR THROUGH OR FROM THE SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TERMS.

13.6 GOOGLE FURTHER EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

14. LIMITATION OF LIABILITY

14.1 SUBJECT TO OVERALL PROVISION IN PARAGRAPH 13.1 ABOVE, YOU EXPRESSLY UNDERSTAND AND AGREE THAT GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS SHALL NOT BE LIABLE TO YOU FOR:

- (A) ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL CONSEQUENTIAL OR EXEMPLARY DAMAGES WHICH MAY BE INCURRED BY YOU, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY.. THIS SHALL INCLUDE, BUT NOT BE LIMITED TO, ANY LOSS OF PROFIT (WHETHER INCURRED DIRECTLY OR INDIRECTLY), ANY LOSS OF

(B) ANY LOSS OR DAMAGE WHICH MAY BE INCURRED BY YOU, INCLUDING BUT NOT LIMITED TO LOSS OR DAMAGE AS A RESULT OF:

(I) ANY RELIANCE PLACED BY YOU ON THE COMPLETENESS, ACCURACY OR EXISTENCE OF ANY ADVERTISING, OR AS A RESULT OF ANY RELATIONSHIP OR TRANSACTION BETWEEN YOU AND ANY ADVERTISER OR SPONSOR WHOSE ADVERTISING APPEARS ON THE SERVICES;

(II) ANY CHANGES WHICH GOOGLE MAY MAKE TO THE SERVICES, OR FOR ANY PERMANENT OR TEMPORARY CESSATION IN THE PROVISION OF THE SERVICES (OR ANY FEATURES WITHIN THE SERVICES);

(III) THE DELETION OF, CORRUPTION OF, OR FAILURE TO STORE, ANY CONTENT AND OTHER COMMUNICATIONS DATA MAINTAINED OR TRANSMITTED BY OR THROUGH YOUR USE OF THE SERVICES;

(IV) YOUR FAILURE TO PROVIDE GOOGLE WITH ACCURATE ACCOUNT INFORMATION;

(V) YOUR FAILURE TO KEEP YOUR PASSWORD OR ACCOUNT DETAILS SECURE AND CONFIDENTIAL;

14.2 THE LIMITATIONS ON GOOGLE'S LIABILITY TO YOU IN PARAGRAPH 14.1 ABOVE SHALL APPLY WHETHER OR NOT GOOGLE HAS BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING.

15. Copyright and trade mark policies

15.1 It is Google's policy to respond to notices of alleged copyright infringement that comply with applicable international intellectual property law (including, in the United States, the Digital Millennium Copyright Act) and to terminating the accounts of repeat infringers. Details of Google's policy can be found at <https://www.google.com/dmca.html>.

15.2 Google operates a trade mark complaints procedure in respect of Google's advertising business, details of which can be found at https://www.google.com/tm_complaint.html.

16. Advertisements

16.1 Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.

16.2 The manner, mode and extent of advertising by Google on the Services are subject to change without specific notice to you.

16.3 In consideration for Google granting you access to and use of the Services, you agree that Google may place such advertising on the Services.

17. Other content

17.1 The Services may include hyperlinks to other web sites or content or resources. Google may have no control over any web sites or resources which are provided by companies or persons other than Google.

17.2 You acknowledge and agree that Google is not responsible for the availability of any such external sites or resources, and does not endorse any advertising, products or other materials on or available from such web sites or resources.

17.3 You acknowledge and agree that Google is not liable for any loss or damage which may be incurred by you as a result of the availability of those external sites or resources, or as a result of any reliance placed by you on the completeness, accuracy or existence of any advertising, products or other materials on, or available from, such web sites or resources.

18. Changes to the Terms

18.1 Google may make changes to the Universal Terms or Additional Terms from time to time. When these changes are made, Google will make a new copy of the Universal Terms available at https://www.google.com/intl/en/chrome/privacy/eula_text.html and any new Additional Terms will be made available to you from within, or through, the affected Services.

18.2 You understand and agree that if you use the Services after the date on which the Universal Terms or Additional Terms have changed, Google will treat your use as acceptance of the updated Universal Terms or Additional Terms.

19. General legal terms

19.1 Sometimes when you use the Services, you may (as a result of, or in connection with your use of the Services) use a service or download a piece of software, or purchase goods, which are provided by another person or company. Your use of these other services, software or goods may be subject to separate terms between you and the company or person concerned. If so, the Terms do not affect your legal relationship with these other companies or individuals.

19.2 The Terms constitute the whole legal agreement between you and Google and govern your use of the Services (but

19.3 You agree that Google may provide you with notices, including those regarding changes to the Terms, by email, regular mail, or postings on the Services.

19.4 You agree that if Google does not exercise or enforce any legal right or remedy which is contained in the Terms (or which Google has the benefit of under any applicable law), this will not be taken to be a formal waiver of Google's rights and that those rights or remedies will still be available to Google.

19.5 If any court of law, having the jurisdiction to decide on this matter, rules that any provision of these Terms is invalid, then that provision will be removed from the Terms without affecting the rest of the Terms. The remaining provisions of the Terms will continue to be valid and enforceable.

19.6 You acknowledge and agree that each member of the group of companies of which Google is the parent shall be third party beneficiaries to the Terms and that such other companies shall be entitled to directly enforce, and rely upon, any provision of the Terms which confers a benefit on (or rights in favor of) them. Other than this, no other person or company shall be third party beneficiaries to the Terms.

19.7 The Terms, and your relationship with Google under the Terms, shall be governed by the laws of the State of California without regard to its conflict of laws provisions. You and Google agree to submit to the exclusive jurisdiction of the courts located within the county of Santa Clara, California to resolve any legal matter arising from the Terms. Notwithstanding this, you agree that Google shall still be allowed to apply for injunctive remedies (or an equivalent type of urgent legal relief) in any jurisdiction.

20. Additional Terms for Extensions for Google Chrome

20.1 These terms in this section apply if you install extensions on your copy of Google Chrome. Extensions are small software programs, developed by Google or third parties, that can modify and enhance the functionality of Google Chrome. Extensions may have greater privileges to access your browser or your computer than regular webpages, including the ability to read and modify your private data.

20.2 From time to time, Google Chrome may check with remote servers (hosted by Google or by third parties) for available updates to extensions, including but not limited to bug fixes or enhanced functionality. You agree that such updates will be automatically requested, downloaded, and installed without further notice to you.

20.3 From time to time, Google may discover an extension that violates Google developer terms or other legal agreements, laws, regulations or policies. Google Chrome will periodically download a list of such extensions from Google's servers. You agree that Google may remotely disable or remove any such extension from user systems in its sole discretion.

21. Additional Terms for Enterprise Use

21.1 If you are a business entity, then the individual accepting on behalf of the entity (for the avoidance of doubt, for business entities, in these Terms, "you" means the entity) represents and warrants that he or she has the authority to act on your behalf, that you represent that you are duly authorized to do business in the country or countries where you operate, and that your employees, officers, representatives, and other agents accessing the Service are duly authorized to access Google Chrome and to legally bind you to these Terms.

21.2 Subject to the Terms, and in addition to the license grant in Section 9, Google grants you a non-exclusive, non-transferable license to reproduce, distribute, install, and use Google Chrome solely on machines intended for use by your employees, officers, representatives, and agents in connection with your business entity, and provided that their use of Google Chrome will be subject to the Terms.

August 12, 2010

Google Chrome Additional Terms of Service

MPEG LA

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PARTNER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEG LA.COM](http://www.mpegla.com).

Adobe

Google Chrome may include one or more components provided by Adobe Systems Incorporated and Adobe Software Ireland Limited (collectively "Adobe"). Your use of the Adobe software as provided by Google ("Adobe Software") is subject to the following additional terms (the "Adobe Terms"). You, the entity receiving the Adobe Software, will be hereinafter referred to as "Sublicensee."

1. License Restrictions.

(a) Flash Player, Version 10.x is designed only as a browser plug-in. Sublicensee may not modify or distribute this Adobe Software for use as anything but a browser plug-in for playing back content on a web page. For example, Sublicensee will not modify this Adobe Software in order to allow interoperation with applications that run outside of the browser (e.g., standalone applications, widgets, device UI).

(b) Sublicensee will not expose any APIs of the Flash Player, Version 10.x through a browser plug-in interface in such a way that allows such extension to be used to playback content from a web page as a stand-alone application.

(c) The Chrome-Reader Software may not be used to render any PDF or EPUB documents that utilize digital rights management protocols or systems other than Adobe DRM.

(d) Adobe DRM must be enabled in the Chrome-Reader Software for all Adobe DRM protected PDF and EPUB documents.

(e) The Chrome-Reader Software may not, other than as explicitly permitted by the technical specifications, disable any capabilities provided by Adobe in the Adobe Software, including but not limited to, support for PDF and EPUB formats and Adobe DRM.

2. Electronic Transmission. Sublicensee may allow the download of the Adobe Software from a web site, the Internet, an intranet, or similar technology (an, "Electronic Transmissions") provided that Sublicensee agrees that any distributions of the Adobe Software by Sublicensee, including those on CD-ROM, DVD-ROM or other storage media and Electronic Transmissions, if expressly permitted, shall be subject to reasonable security measures to prevent unauthorized use. With relation to Electronic Transmissions approved hereunder, Sublicensee agrees to employ any reasonable use restrictions set by Adobe, including those related to security and/or the restriction of distribution to end users of the Sublicensee Product.

3. EULA and Distribution Terms.

(a) Sublicensee shall ensure that the Adobe Software is distributed to end users under an enforceable end user license agreement, in favor of Sublicensee and its suppliers containing at least each of the following minimum terms (the "End-User License"): (i) a prohibition against distribution and copying, (ii) a prohibition against modifications and derivative works, (iii) a prohibition against decompiling, reverse engineering, disassembling, and otherwise reducing the Adobe Software to a human-perceivable form, (iv) a provision indicating ownership of Sublicensee Product (as defined in Section 8) by Sublicensee and its licensors, (v) a disclaimer of indirect, special, incidental, punitive, and consequential damages, and (vi) other industry standard disclaimers and limitations, including, as applicable: a disclaimer of all applicable statutory warranties, to the full extent allowed by law.

(b) Sublicensee shall ensure that the Adobe Software is distributed to Sublicensee's distributors under an enforceable distribution license agreement, in favor of Sublicensee and its suppliers containing terms as protective of Adobe as the Adobe Terms.

4. Opensource. Sublicensee will not directly or indirectly grant, or purport to grant, to any third party any rights or immunities under Adobe's intellectual property or proprietary rights that will subject such intellectual property to an open source license or scheme in which there is or could be interpreted to be a requirement that as a condition of use, modification and/or distribution, the Adobe Software be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; or (iii) redistributable at no charge. For clarification purposes, the foregoing restriction does not preclude Sublicensee from distributing, and Sublicensee will distribute the Adobe Software as bundled with the Google Software, without charge.

5. Additional Terms. With respect to any update, upgrade, new versions of the Adobe Software (collectively "Upgrades") provided to Sublicensees, Adobe reserves the right to require additional terms and conditions applicable solely to the Upgrade and future versions thereof, and solely to the extent that such restrictions are imposed by Adobe on all licensees of such Upgrade. If Sublicensee does not agree to such additional terms or conditions, Sublicensee will have no license rights with respect to such Upgrade, and Sublicensee's license rights with respect to the Adobe Software will terminate automatically on the 90th day from the date such additional terms are made available to Sublicensee.

6. Proprietary Rights Notices. Sublicensee shall not, and shall require its distributors not to, delete or in any manner alter the copyright notices, trademarks, logos or related notices, or other proprietary rights notices of Adobe (and its licensors, if any) appearing on or within the Adobe Software or accompanying materials.

7. Technical Requirements. Sublicensee and its distributors may only distribute Adobe Software and/or Upgrade on devices that (i) meet the technical specifications posted on <http://www.adobe.com/mobile/licensees>, (or a successor web site thereto), and (ii) has been verified by Adobe as set forth below.

8. Verification and Update. Sublicensee must submit to Adobe each Sublicensee product (and each version thereof) containing the Adobe Software and/or Upgrade ("Sublicensee Product") that do not meet the Device Verification exemption criteria to be communicated by Google, for Adobe to verify. Sublicensee shall pay for each submission made by Sublicensee by procuring verification packages at Adobe's then-current terms set forth at <http://flashmobile.adobe.com/>. Sublicensee Product that has not passed verification may not be distributed. Verification will be accomplished in accordance with Adobe's then-current process described at <http://flashmobile.adobe.com/> ("Verification").

9. Profiles and Device Central. Sublicensee will be prompted to enter certain profile information about the Sublicensee Products either as part of the Verification process or some other method, and Sublicensee will provide such information, to Adobe. Adobe may (i) use such profile information as reasonably necessary to verify the Sublicensee Product (if such product is subject to Verification), and (ii) display such profile information in "Adobe Device Intelligence system," located at <https://devices.adobe.com/partnerportal/>, and made available through Adobe's

10. Export. Sublicensee acknowledges that the laws and regulations of the United States restrict the export and re-export of commodities and technical data of United States origin, which may include the Adobe Software. Sublicensee agrees that it will not export or re-export the Adobe Software, without the appropriate United States and foreign governmental clearances, if any.

11. Technology Pass-through Terms.

(a) Except pursuant to applicable permissions or agreements therefor, from or with the applicable parties, Sublicensees shall not use and shall not allow the use of, the Adobe Software for the encoding or decoding of mp3 audio only (.mp3) data on any non-pc device (e.g., mobile phone or set-top box), nor may the mp3 encoders or decoders contained in the Adobe Software be used or accessed by any product other than the Adobe Software. The Adobe Software may be used for the encoding or decoding of MP3 data contained within a swf or flv file, which contains video, picture or other data. Sublicensee shall acknowledge that use of the Adobe Software for non-PC devices, as described in the prohibitions in this section, may require the payment of licensing royalties or other amounts to third parties who may hold intellectual property rights related to the MP3 technology and that Adobe nor Sublicensee has not paid any royalties or other amounts on account of third party intellectual property rights for such use. If Sublicensee requires an MP3 encoder or decoder for such use, Sublicensee is responsible for obtaining the necessary intellectual property license, including any applicable patent rights.

(b) Sublicensee will not use, copy, reproduce and modify (i) the On2 source code (provided hereunder as a component of the Source Code) as necessary to enable the Adobe Software to decode video in the Flash video file format (.flv or .f4v), and (ii) the Sorenson Spark source code (provided hereunder as a component of the Source Code) for the limited purpose of making bug fixes and performance enhancements to the Adobe Software. All codecs provided with the Adobe Software may only be used and distributed as an integrated part of the Adobe Software and may not be accessed by any other application, including other Google applications.

(c) The Source Code may be provided with an AAC codec and/or HE-AAC codec ("the AAC Codec"). Use of the AAC Codec is conditioned on Sublicensee obtaining a proper patent license covering necessary patents as provided by VIA Licensing, for end products on or in which the AAC Codec will be used. Sublicensee acknowledges and agrees that Adobe is not providing a patent license for an AAC Codec under this Agreement to Sublicensee or its sublicensees.

(d) THE SOURCE CODE MAY CONTAIN CODE LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR WILL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. See <http://www.mpegla.com>

12. Update. Sublicensee will not circumvent Google's or Adobe's efforts to update the Adobe Software in all Sublicensee's products incorporating the Adobe Software as bundled with the Google Software ("Sublicensee Products").

13. Attribution and Proprietary Notices. Sublicensee will list the Adobe Software in publicly available Sublicensee Product specifications and include appropriate Adobe Software branding (specifically excluding the Adobe corporate logo) on the Sublicensee Product packaging or marketing materials in a manner consistent with branding of other third party products contained within the Sublicensee Product.

14. No Warranty. THE ADOBE SOFTWARE IS MADE AVAILABLE TO SUBLICENSEE FOR USE AND REPRODUCTION "AS IS" AND ADOBE MAKES NO WARRANTY AS TO ITS USE OR PERFORMANCE. ADOBE AND ITS SUPPLIERS DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS OBTAINED BY USING THE ADOBE SOFTWARE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO SUBLICENSEE IN SUBLICENSEE'S JURISDICTION, ADOBE AND ITS SUPPLIERS MAKE NO WARRANTIES, CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING WITHOUT LIMITATION NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, SATISFACTORY QUALITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. SUBLICENSEE AGREES THAT SUBLICENSEE SHALL NOT MAKE ANY WARRANTY, EXPRESS OR IMPLIED, ON BEHALF OF ADOBE.

15. Limitation of Liability. IN NO EVENT WILL ADOBE OR ITS SUPPLIERS BE LIABLE TO SUBLICENSEE FOR ANY DAMAGES, CLAIMS OR COSTS WHATSOEVER OR ANY CONSEQUENTIAL, INDIRECT, OR INCIDENTAL DAMAGES, OR ANY LOST PROFITS OR LOST SAVINGS, EVEN IF AN ADOBE REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS, DAMAGES, CLAIMS OR COSTS OR FOR ANY CLAIM BY ANY THIRD PARTY. THE FOREGOING LIMITATIONS AND EXCLUSIONS APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW IN SUBLICENSEE'S JURISDICTION. ADOBE'S AGGREGATE LIABILITY AND THAT OF ITS SUPPLIERS UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO ONE THOUSAND DOLLARS (US\$1,000). Nothing contained in this Agreement limits Adobe's liability to Sublicensee in the event of death or personal injury resulting from Adobe's negligence or for the tort of deceit (fraud). Adobe is acting on behalf of its suppliers for the purpose of disclaiming, excluding and/or limiting obligations, warranties and liability as provided in this Agreement, but in no other respects and for no other purpose.

16. Content Protection Terms

“Compliance and Robustness Rules” means the document setting forth compliance and robustness rules for the Adobe Software located at <http://www.adobe.com/mobile/licensees>, or a successor web site thereto.

“Content Protection Functions” means those aspects of the Adobe Software that are designed to ensure compliance with the Compliance and Robustness Rules, and to prevent playback, copying, modification, redistribution or other actions with respect to digital content distributed for consumption by users of the Adobe Software when such actions are not authorized by the owners of such digital content or its licensed distributors.

“Content Protection Code” means code within certain designated versions of the Adobe Software that enables certain Content Protection Functions.

“Key” means a cryptographic value contained in the Adobe Software for use in decrypting digital content.

(b) License Restrictions. Sublicensee’s right to exercise the licenses with respect to the Adobe Software is subject to the following additional restrictions and obligations. Sublicensee will ensure that Sublicensee’s customers comply with these restrictions and obligations to the same extent imposed on Sublicensee with respect to the Adobe Software; any failure by Sublicensee’s customers to comply with these additional restrictions and obligations shall be treated as a material breach by Sublicensee.

b.1. Sublicensee and customers may only distribute the Adobe Software that meets the Robustness and Compliance Rules as so confirmed by Sublicensee during the verification process described above in the Adobe Terms.

b.2. Sublicensee shall not (i) circumvent the Content Protection Functions of either the Adobe Software or any related Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software or (ii) develop or distribute products that are designed to circumvent the Content Protection Functions of either the Adobe Software or any Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software.

(c) The Keys are hereby designated as Adobe’s Confidential Information, and Sublicensee will, with respect to the Keys, adhere to Adobe’s Source Code Handling Procedure (to be provided by Adobe upon request).

(d) Injunctive Relief. Sublicensee agrees that a breach of this Agreement may compromise the Content Protection Functions of the Adobe Software and may cause unique and lasting harm to the interests of Adobe and owners of digital content that rely on such Content Protection Functions, and that monetary damages may be inadequate to compensate fully for such harm. Therefore, Sublicensee further agrees that Adobe may be entitled to seek injunctive relief to prevent or limit the harm caused by any such breach, in addition to monetary damages.

17. Intended Third-party Beneficiary. Adobe Systems Incorporated and Adobe Software Ireland Limited are the intended third-party beneficiaries of Google’s agreement with Sublicensee with respect to the Adobe Software, including but not limited to, the Adobe Terms. Sublicensee agrees, notwithstanding anything to the contrary in its agreement with Google, that Google may disclose Sublicensee’s identity to Adobe and certify in writing that Sublicensee has entered into a license agreement with Google which includes the Adobe Terms. Sublicensee must have an agreement with each of its licensees, and if such licensees are allowed to redistribute the Adobe Software, such agreement will include the Adobe Terms.

[Printer-friendly version](#)

Note: Installing Google Chrome will **add the Google repository** so your system will automatically keep Google Chrome up to date. If you don’t want Google’s repository, do “sudo touch /etc/default/google-chrome” before installing the package.

☒ Set Google Chrome as my default browser

☒ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. [Learn more](#)

Accept and Install 

Download Chrome

Download for Windows

For Windows 10/8.1/8/7 32-bit

For Windows 10/8.1/8/7 64-bit

This computer will no longer receive Google Chrome updates because Windows XP and Windows Vista are no longer supported.

Download for Mac

Mac OS X 10.10 or later

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

This computer will no longer receive Google Chrome updates because Mac OS X 10.6 - 10.9 are no longer supported.

Debian/Ubuntu/Fedora/openSUSE

Download for phone or tablet

- [Android](#)
- [iOS](#)

Download for another desktop OS

- [Windows 10/8.1/8/7 64-bit](#)
- [Windows 10/8.1/8/7 32-bit](#)
- [Mac OS X 10.10 or later](#)
- [Linux](#)

Frozen versions

- [Windows XP](#)
- [Windows Vista](#)
- [Mac 10.6 - 10.8](#)
- [Mac 10.9](#)